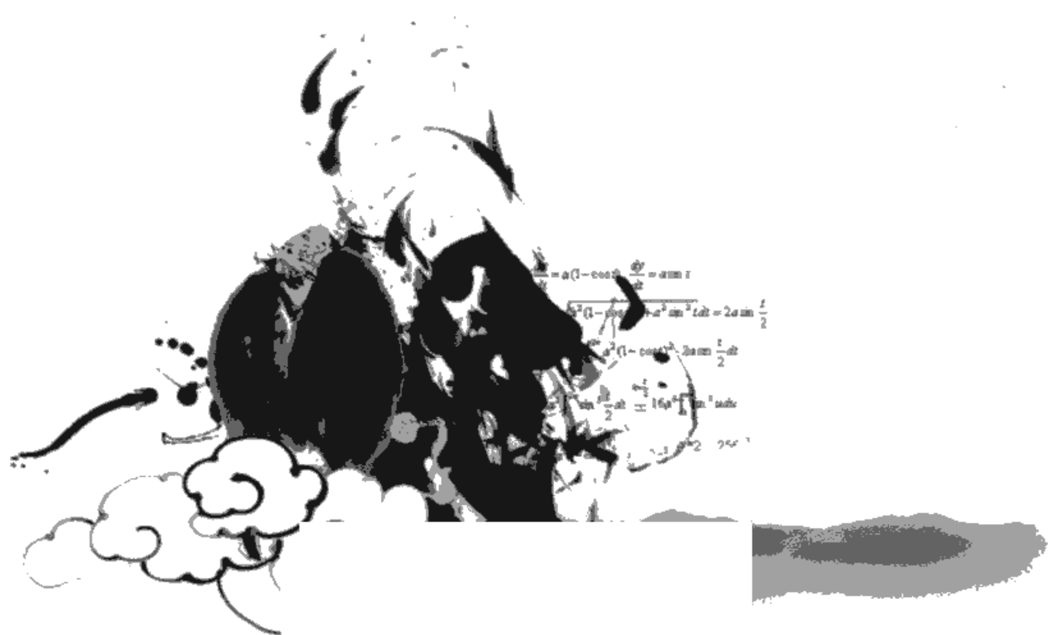
"十一五"国家重点图书出版规划项目

科学素养大家谈丛书





当代数学史话

张奠宙 王善平 编著



大连理工大学出版社
DALIAN UNIVERSITY OF TECHNOLOGY PRESS



当代数学史话

HISTORIC STORIES OF MODERN MATHEMATICS

数学无疑起源于古人对于现实世界的经验和认识，但经过数千年的曲折发展，它已经成为一门独立于现实世界、具有严密的思想和方法、高度抽象的人类重要知识体系；另一方面，数学依然在现实世界以及人类其他学科领域中有着广泛应用。

20世纪的数学，已经渗透到人类生活的各个领域，以前所未有的方式影响着人类对世界、对自身的看法。回顾这100年的数学发展，是如此的波澜壮阔、丰富多彩，远远超出了世纪之初任何人之想象。从本书中我们不仅可以看到百年数学的万千气象，更能感受到其中的智慧、合作与尊重。

——张奠宙　王善平

ISBN 978-7-5611-4640-8



上架建议：科普读物

定价：30.00元

图书在版编目(CIP)数据

当代数学史话/张奠宙,王善平编著.一大连:大连理工大学出版社,2010.1

(科学素养大家谈丛书)

ISBN 978-7-5611-4640-8

Ⅰ.当… Ⅱ.①张…②王… Ⅲ.数学—普及读物 Ⅳ.O1-49

中国版本图书馆 CIP 数据核字(2009)第 067500 号

大连理工大学出版社出版

地址:大连市软件园路 80 号 邮政编码:116023

发行:0411-84708842 邮购:0411-84703636 传真:0411-84701466

E-mail:dutp@dutp.cn URL:http://www.dutp.cn

大连美跃彩色印刷有限公司印刷 大连理工大学出版社发行

幅面尺寸:147mm×210mm 印张:10.5 字数:210 千字

2010 年 1 月第 1 版 2010 年 1 月第 1 次印刷

责任编辑:刘新彦 王 伟 责任校对:知 轩

封面设计:李昕阳

ISBN 978-7-5611-4640-8 定价:30.00 元

读书面面观

——雷声隆隆，光照天地[1]

你最喜爱什么？——书籍。

你经常去哪里？——书店。

你最大的兴趣是什么？——读书。

这是友人提出的问题和我的回答。真的，我这一辈子算是和书籍，特别是好书结下了不解之缘。有人说，读书要费那么大的劲，又发不了财，读它做什么？我却至今不悔；不仅不悔，反而情趣越来越浓。想当年，我也曾爱打球，也曾爱下棋，对操琴也有兴趣，还登台伴奏过。但后来却都一一断交，“终身不复鼓琴”。那原因，便是怕花费时间，玩物丧志，误了我的大事——求学。这当然过激了一些，有点

---

① 原载《东南电大学报》，1990年第1期。经王梓坤教授提议，作为本套丛书的序言。

"左"。剩下来惟有读书一事，自幼至今，无日少废，谓之书痴也可，谓之书橱也可，管它呢，人各有志，不可相强。我的一生大志，便是教书，而当教师，不多读书是不行的。

学生读书，应付考试是一大目的。为考试而读，自然是一苦事。不考又怎么行呢？不过，如果考试成绩好，可以帮助我们升学，越升越高，越学越深。考试还可以强迫我们学一些难学但又不能不学的知识。而培根说："知识就是力量。"所以，考试也有积极的一面，不能太多地说它的坏话。

如果把读书只看成是"学而优则仕"的手段，那未免太偏颇了。其实读书的意义远远在此之上。读好书是一种乐趣，一种情操，一种向全世界古往今来的伟人和名人求教的方法，一种和他们展开讨论的方式，一封出席各种场合、体验各种生活、结识各种人物的邀请信，一张迈进科学宫殿和未知世界的入场券，一股改造自己、丰富自己的强大力量。书籍是全人类有史以来共同创造的财富，是永不枯竭的智慧的泉源。失意时读书，可以使人重振旗鼓；得意时读书，可以使人头脑清醒；疑难时读书，可以得到解答或启示；年轻人读书，可明奋进之道；年老人读书，能知健神之理。浩浩乎！洋洋乎！如临大海，或波涛汹涌，或清风微拂，取之不尽，用之不竭。吾于读书，无疑义矣，三日不读，则头脑麻木，心摇摇无主。

潜能需要激发

我和书籍结缘，开始于一次非常偶然的机会。大概是八九岁吧，家里穷得揭不开锅，我每天从早到晚，都要去田园里帮工。一天，偶然从旧木柜阴湿的角落里，找到一本腊光纸的小书，像袖珍字典那么大，自然很破了。屋内光线暗淡，又是黄昏时分，只好拿到大门外去看。封面已经脱落，扉页上写的是《薛仁贵征东》。管它呢，且往下看。第一回的标题已忘记，只是那首开卷诗不知为什么至今仍记忆犹新：

日出遥遥一点红，
飘飘四海影无踪。
三岁孩童千两价，
保主跨海去征东。

第一句指山东，二、三两句分别点出薛仁贵（雪，人贵）。那时识字很少，半看半猜，居然引起了我极大的兴趣，同时也教我认识了许多生字。这是我有生以来独立看的第一本书。尝到甜头以后，我便千方百计去找书，向小朋友借，到亲友家找，居然断断续续看了《薛丁山征西》、《彭公案》、《二度梅》等等。樊梨花便成了我心中的女英雄。后来认字越来越多，胃口越来越大，居然又读了《三国演义》、《东周列国志》、《西游记》、《民国通俗演义》，甚至《聊斋志异》。只是《红楼梦》没有读完，因为里面没有打仗。我开始向村里人

讲故事了，大讲“孔明借箭”、“荆轲刺秦王”，大人们惊奇的眼光极大地鼓励了我，原来世界上有这么多有趣的书，我真入迷了。从此，放牛也罢，车水也罢，我总要带一本书，而且还练出了边走田间小路边读书的本领，读得津津有味，不知人间别有他事。

当我们安静下来回想往事时，往往会发现一些偶然的小事却影响了自己的一生。如果不是找到那本《薛仁贵征东》，我的好学心也许激发不起来，我这一生，也许会走另一条路。人的潜能，好比一座汽油库，星星之火，可以使它雷声隆隆、光照天地；但若少了这粒火星，它便会成为一潭死水，永归沉寂。所以我想，给孩子们看一点有趣而又有益的小说、童话，可以培养他们读书的兴趣。可惜现在为了追求升学率，功课排得那么紧，加上社会上又有那么多不健康因素的引诱，他们哪有时间去自由阅读呢？

抄，总抄得起

好容易上了中学，做完功课还有点时间，便常光顾图书馆，假日也全用来读书。好书借了实在舍不得还，但买不到也买不起，便下决心动手抄。抄，总抄得起。我抄过林语堂写的《高级英文法》，抄过英文本的《英文典大全》，还抄过《孙子兵法》。这本书实在爱得狠了，竟一口气抄了两份，另一份送给好友，劝他也读一点兵书。人们但知抄书之苦，未知抄书之益，抄完毫末俱见，一览无余，胜读十遍。

读高中时，居然找到了列宁写的几本小册子。那时还没解放，列宁的大名偶尔听到，但神秘得很，越神秘就越想偷尝禁果。虽然不懂他讲的大道理，却多少感到列宁在替穷人说话，便自然赞成他。这是我读革命书籍的开始。

我考试的成绩不算坏，这与喜欢读课外参考书有关。每门课，除了在教本上下大工夫以外，总要找到一两本同类的参考书对着看。对照之下，常能加深理解，并扩大知识面。但做习题，却决不轻易看别人的解答。有时一道题折磨我两三天，气得火星直冒，也不妥协。苦头确实吃了不少，但本领也多少练了些出来，这对后来的科研工作有所裨益。做习题也可以看成小小的科研，只不过做的是别人已做过的现成题，而科研则是自己出题（或任务出题）自己做，前人从未做过而已。

回想起来，自学和做题（或做实验）这两件事，对我后来的工作起着极重要的作用。通过自学猎取知识，通过做题锻炼才能。知识与才能是两回事，有知识未必有才能；另一方面，没有知识也就谈不上才能，特别是在科学发达的今天。美国前总统杜鲁门说："历史使我知道，任何一个国家的领导人为了负起领导的重担，必须懂得历史，不仅要懂得本国史还要懂得所有大国的历史。"可见知识对于才能的重要。

如何自学一门新课程

培养自学能力，谈何容易。自学一部小说，一本通俗杂志，固然不成问题；但若要自学一门从未学过的硬科学，譬如说微积分，那便非常困难。没有足够的基础、毅力和勤奋，是不可能学好的。

首先，要选一本好的微积分教材。这本书，第一，既概括了这门课程的主要内容，又非枝蔓丛生、繁杂冗长、浪费读者的精力；第二，定义、定理和证明准确无误，而且能从多种证明中挑出有启发性的好证明，叙述也清晰易懂；第三，内容不是材料的堆砌，也不只是逻辑的演绎，而应富于思想性，给读者以智慧；最后，有适量的习题，由易而难，逐步训练读者的能力。

其次，要耐心地精读细读。读过序言和目录后，就要安下心来。从第一页起一行一行地读，切忌冒进。很可能在某一处用到另一件事或另一定理，必须追根溯源，弄清楚再往下看。每条定理的条件、证明和结论，都必须看懂。这样，读起来就非常之慢，每天能读懂一两页，就算很有收获了。如果卡在某一处，费了很大的力气，还是不懂，那就只好暂时跳过去，反正我对它已有很深的印象，迟早总要弄懂的。但这种跳跃，切勿太多。俄国著名生理学家巴甫洛夫告诫青年，读书要循序渐进，循序渐进，最后还是循序渐进。

华罗庚先生也多次强调循序渐进的重要性。我们的思想往往急于求成。控制自己稳步前进的好方法是边读边做笔记，一动手就会发现许多问题，动脑加动手，实是精读的好方法。例题要细看，因为定理是抽象的，例题是具体的，而抽象寓于具体之中。多记住例题，不仅可加深理解，而且有助于日后的科研，读完一节或一章，必须做完书上的习题。这样一章一章地读下去，待读完全书，我们对此书的内容已了解大半。不过还只停留在"局部"读的阶段，对各定理间、各章节间的关系还不太清楚，何况还留下一些未解决的问题。这意味着，要及时再细读第二遍。这一遍除起复习作用外，重点应放在还未看懂的地方，并尽量找出相互之间的关系。这就是说，我们已开始"整体"地读。第一遍留下来的问题，这次可以解决一大部分，为什么？因为这时的我，已非前时的我，我现在的水平，已由于通读了第一遍提高了不少。如此通读几遍，最后一两遍应倒过来读，即从最后一章倒读回去，这更有助于弄清全书的脉络。至此，对全书已很了解，发现很长的推理证明其实只有几个要点，全书也只有几个高潮，其他无非是外围。把书合上，我也能说出它的骨架，已达到庄子所说"目无全牛"的境界。不仅读书如此，做其他事情也是如此。任何很复杂的事物，只有在头脑中变得很简单时，才能抓住关键，才能记住它，把握它，改造它和利用它。

第三，自学并非绝对排斥外援，在充分准备的基础上，请老师指出重点，或进行重点讨论，都是有益的。

两种循环与两极分化

甲、乙两人同时考入大学，水平相差无几，但到毕业时，却相距很大，甲几乎可以当乙的老师。原因何在呢？

原因可能很多，我们只从学习方法的角度来讨论。众所周知，一门课教学的基本程序是：上课、复习、做习题（或做实验），三个环节不断循环。我多年观察，循环有良性和恶性两种。

上课前，甲进行了预习，他已大致了解老师下节课要讲的内容，也知道哪些是难点，哪里是自己没有看懂的地方。于是上课听讲时，他心中有数，对已看懂的，再听一遍，可起复习巩固作用，对未看懂的，便集中精力、全神贯注地去听。由于有的放矢，他可以把难点基本上消灭在课堂上，同时也搞清了自己课前没有看懂的原因，从而不知不觉地提高了自学能力，这一收获甚至比克服当前的难点更重要。由于听课效率高，课后复习的时间便少，做习题也快，这样又争取到了预习下次课的时间，下一堂课又听得好……如此继续，是谓良性循环。

乙则不然，他没有预习，上课时完全被动，许多地方没有听懂，复习时间多，习题做不完，功课越堆越多，学习越来越困难，他卷入了恶性循环。

正是这两种循环，如同两辆分岔而行的汽车，把他们的水平差距越拉越大。怎样才能进入良性循环？关键在于课前预习。请抓住空暇时间和假日，预习一门或两门课吧！并不一定全看完，也不一定全看懂，这对于你的学习大有好处。时间是挤出来的，如果下定决心，持之以恒，就必定能做到。

始于精于一，返于精于博

关于康有为的教学法，他的弟子梁启超说："康先生之教，特标专精、涉猎二条，无专精则不能成，无涉猎则不能通也。"可见康有为强烈要求学生把专精和广博（即"涉猎"）相结合。鲁迅也劝青年："应做的功课已完而有余暇，大可以看看各样的书，即使和本业毫不相干的，也要泛览。譬如学理科的，偏看看文学书，学文学的，偏看看科学书，看看别个在那里研究的，究竟是怎么一回事。这样子，对于别人、别事，可以有更深的了解。"

在先后次序上，我认为要从"精于一"开始。首先应集中精力学好专业，并在专业的科研中作出成绩，然后逐步扩大领域，力求多方面的精。简言之，即"始于精于一，返于精于博"。正如中国革命一样，必须先有一块根据地，站稳后再开创几块，最后连成一片。

这里有两种偏向。一是对专业漫不经心，这山看着那山高，什么控制论、外星人、宇宙论、新思维，都知道一点，夸

夸其谈,眼高手低,回过头来却看不起自己的专业,认为那不过是雕虫小技,没多大意思。就好像逛过花花世界的人,瞧不起自己的家乡一样。这样下去,必将一无所成。另一种是终身只守住专业中一小角落,其他的科学进展、世界形势,甚至自己专业的近邻,一律不闻不问。长此以往,很可能思想枯竭,性情乖僻。

许多大家都是走先精后博、由博返精的道路的。一条路走通了,就可触类旁通地走其他的路;而走了其他的路,又可回过头来看原来的路,相互比较,容易受到新的启发,导致新的发现。

丰富我文采,澡雪我精神

辛苦了一周,人相当疲劳了,每到星期六晚,我便到旧书店走走,这已成为生活中的一部分,多年如此。一次,偶然看到一套《纲鉴易知录》,编者之一便是选编《古文观止》的吴楚材。这部书提纲挈领地讲中国历史,上自盘古氏,直到明末,记事简明,文字古雅,又富于故事性。那时正值"文革",我自愧无打砸抢之才,不必夜间出去打家劫舍,便把这部书从头到尾读了一遍,不想它大大开拓了我的眼界,启发了我读史书的兴趣。随后又读了《后汉书》中的"党锢列传"。这篇文章讲的是东汉名士与宦官的斗争,一些正人君子被宦官害得家破人亡。联想到当时实际,许多老革命和专家学者惨遭迫害,这不基本上是历史的重演吗?读史提

高了我的认识，使我对“文革”的实质一开始就比较清楚，免去了日后的许多麻烦。

我爱读中国的古典小说，例如《三国演义》和《东周列国志》。我常对人说，这两部书简直是世界上政治阴谋诡计大全。即使近年来极时髦的人质问题（伊朗人质、劫机人质等），这些书中早就有了，秦始皇的父亲便是受害者，堪称为“人质之父”。

《庄子》超尘绝俗，不屑于名利，而名利正是使聪明人上钩之饵；其中“秋水”、“解牛”诸篇，诚绝唱也。《论语》束身严谨，勇于面世，“己所不欲，勿施于人”、“躬自厚而薄责于人”，有长者之风。司马迁的《报任少卿书》，读之我心两伤，既伤少卿，又伤司马；我不知道少卿是否收到这封信，有何感想，希望有人作点研究。我也爱读鲁迅的杂文，果戈理、梅里美的小说。我非常敬重文天祥、秋瑾的人品，常记他们的诗句“人生自古谁无死，留取丹心照汗青”、“谁言女子非英物，夜夜龙泉壁上鸣”。唐诗宋词、《西厢记》、《牡丹亭》，丰富我文采，澡雪我精神，其中精粹，实是人间神品。元朝王冕的诗句“花落不随流水去，鹤归常伴白云来”，使人悠然神往。读了邓拓的《燕山夜话》，既叹服其广博，也使我动了写《科学发现纵横谈》之心。不料这本小册子竟给我招来了上千封鼓励信，无他，时势造作品而已。原来“文革”十年，到处是“万岁万万岁”的陈词滥调，人们在精神窒息中渴望

新鲜文风，这本小册子在一定程度上迎合了这种要求，以后便出现了许许多多的“纵横谈”。

从学生时代起，我就喜读方法论方面的论著。我想，做什么事情都要讲究方法，追求效率、效果和效益，方法好能事半功倍。《孙子兵法》启发了我：连打仗这样复杂而紧迫的事都有方法可循，其他事就该更有方法了。于是我很留心一些著名科学家、文学家写的心得体会和经验。我曾惊讶为什么巴尔扎克在50年短短的一生中能写出上百本书，并从他的传记中去寻找答案。我也奇怪26岁的诸葛亮能在刘备三顾茅庐时发表著名的“隆中对”，对天下大事了如指掌，并确定了以后的战略方针。须知那时他住在穷乡僻壤，既无报纸杂志，也无广播电视。系统地给我以科学史知识的是贝尔纳著的《历史上的科学》、霍利切尔的《科学世界图景中的自然界》、《爱因斯坦文集》等书。此外，恩格斯的《自然辩证法》、海森堡的《物理学与哲学》、薛定谔的《生命是什么》、康德的《宇宙发展史概论》、梅特里的《人是机器》、莫诺的《偶然性与必然性》、怀特海的《科学与近代世界》、维纳的《控制论》、罗素的《西方哲学史》、普里戈金等的《从混沌到有序》，以及阿西莫夫等人的优秀科普作品，都是给人知识、增人智慧的好书。文史哲和科学的海洋无边无际，先哲们明智之光沐浴着人们的心灵，我衷心感谢他们的恩惠。

读书的另一面

以上我谈了读书的好处，怎样攻读专业书以及阅读其他书，讲了精与博的关系，为书籍说了许多好话。然而世界上每件事都有一个限度，过了限就要出毛病，读书也不例外。所以我要回过头来说说事情的另一面。

读书要选择。世上有各种各样的书：有的不值一看，有的只值看20分钟，有的可看5年，有的可保存一辈子，有的将永远不朽。即使是不朽的超级名著，由于我们的精力与时间有限，也必须加以选择。决不要看坏书。对一般书，要学会速读。古人说，一目十行。今天看来，这速度不能算快，必须在一小时内就可大致看完一本500页的书，说出它的主要内容和精华。据说美国前总统肯尼迪就有这种本领。这样，我们才能赢得时间去读好书，特别是读经过历史考验的名著。对名著，读一遍是不够的，隔一段时间重读，会有新的体会。托马斯·霍布斯(1588—1679)只阅读非常杰出的著作，他甚至经常说，如果他也像其他学者那样阅读那么多的书，他就会与他们一样无知了。这话说得不够客气，但他读书注意选择，却是很对的。

读书要多思考。读书时，我们的大脑基本上被书本占据，成为作者驰骋的场所。如果我们不积极思考，大脑便出租给作者了，任凭他的马队去践踏，久而久之，会伤害自己

的思维能力。要知道,书本无非是作者的一篇有准备的长篇发言,由于他有充分准备,所以合理的地方比较多,但绝非完美无缺。应该想想,他说得对吗?完全吗?适合今天的情况吗?从书本中迅速获得效果的好办法是有的放矢地读书,带着问题去读,或偏重某一方面去读。这时我们的思维处于主动寻找的地位,就像猎人追找猎物一样主动,很快就能找到答案,或者发现书中的问题。所谓"偏重一方面去读",是苏轼提倡的读书方法。例如读《红楼梦》,第一遍读可偏重其中人际关系,第二遍可偏重景物描写,第三遍可注意当时的饮食和医药,等等。每读一遍,深入一面,甚至可以写成一篇论文呢。

有的书浏览即止,有的要读出声来,有的要心头记住,有的要笔头记录。对重要的专业书或名著,要勤做笔记,"不动笔墨不读书"。动脑加动手,手脑并用,既可加深理解,又可避忘备查。特别是自己的灵感,更要及时抓住。清代章学诚在《文史通义》中说:"札记之功必不可少,如不札记,则无穷妙绪,如雨珠落大海矣。"许多大事业、大作品,都是长期积累和短期突击相结合的产物。涓涓不息,将成江河;无此涓涓,何来江河?

爱好读书是许多伟人的共同特性,不仅学者专家如此,一些大政治家、大军事家也如此。曹操、康熙、拿破仑、毛泽东都是手不释卷、嗜书如命的人。毛泽东只念过中等师范,

却领导了中国革命，而且文史哲都达到很高水平。《沁园春·雪》一词，千古独步，这些都与他毕生刻苦自学密切相关。

序

一部近代世界史表明：凡是世界经济、军事大国，一定也是数学强国。17 世纪的英国产业革命，牛顿的微积分诞生在英伦三岛。18 世纪法国大革命催生拿破仑帝国，法国数学学派称雄欧洲。19 世纪中叶，德国资产阶级崛起，数学王子高斯带来德国数学的辉煌。到了 20 世纪的伊始，国际数学界形成法国与德国数学争雄的格局。那时的美国尚未称霸世界，数学也处于二流水平。至于 20 世纪的中叶以后，则是美国数学与苏联数学对决的年代了。清代学者赵翼有诗云："江山代有才人出，各领风骚数百年。"在数学界，能领先数百年是不可能的，能当几十年的霸主就很不容易了。

1900 年，第二次国际数学家大会在巴黎召开。法国的庞加莱任大会主席，德国的希尔伯特作大会报告。这反映了法、德两国在国际数学的领导地位依然平分秋色。庞加莱是一位牛顿式数学家，关注天文学、物理学等自然科学中的数学问题，开创了

定性理论、拓扑学等许多影响深远的新学科。希尔伯特也是一位全才的数学大师，曾有证据显示他和爱因斯坦独立地提出了相对论。不过，希尔伯特更以纯粹数学的创见、提倡形式主义的数学哲学而著称，可以说更具欧几里得那样的古希腊数学的特色。

希尔伯特赢得了很高的声誉。他在大会上提出了20世纪将要解决的23个问题，引无数英雄竞折腰。能够解决其中一个问题都是极高的荣誉（著名的哥德巴赫猜想是第8个问题的一部分）。希尔伯特引导的现代公理化数学思潮，成为人类数学文明的又一个高峰。

庞加莱于1912年去世。法国数学渐渐走下坡路。不久前披露的档案表明，鉴于庞加莱的数学工作大气磅礴，在证明的严密性上有时不甚讲究，法国同行（包括他的导师毕卡）颇有非议。结果是权威的领导决定不让庞加莱教数学课，只能教天文学和物理学。1920年代的法国数学，逐渐远离庞加莱的数学路线，研究领域缩小在纯粹数学的一个狭小领域，简直成了"函数论王国"。于是一批年轻的数学家从1920年代开始，向格丁根学派学习，继承发扬希尔伯特的数学传统，努力走出函数论王国的圈子。这就是著名的布尔巴基学派。20世纪法国数学的这一亮点，却是德国希尔伯特形式主义的时尚。布尔巴基学派的结构主义的数学，曾经在1950年代前后领导世界数学潮流，风靡一时。

20世纪的前30年，世界数学中心在德国的格丁根大学。那里曾是高斯、黎曼等大家工作的地方，后来则是以希尔伯特为首

的格丁根数学学派大本营。爱因斯坦发表相对论时，这里的闵可夫斯基就发展四维的时空几何。量子力学刚刚形成，外尔的《量子力学数学基础》立即在格丁根问世。当过希尔伯特助教的冯·诺依曼，则建立起希尔伯特空间上的算子谱论，成为量子力学的数学框架。迄今为止最伟大的女数学家E·诺特在这里发表影响深远的"一般理想论"，开抽象代数的先河。那时的欧洲，还从未有过女性教授。希尔伯特为此忿忿不平："大学评议会不是浴室，为什么不准妇女进入？"

1933年的那个黑色的春天，立即把格丁根的辉煌葬送了。希特勒法西斯上台迫害犹太人，驱逐犹太籍的科学家。爱因斯坦是犹太人，冯·诺依曼、诺特都是犹太人，外尔的太太是犹太人，格丁根数学研究所的所长柯朗也是犹太人。他们先后被迫到达美国的普林斯顿和纽约，美国也因此成为新的世界数学中心。

在20世纪初，像爱迪生那样的美国发明家领导着先进技术的世界潮流，经济实力已经居世界前列。但是基础科学的水平还远落在欧洲后面。美国学生到欧洲学习数学，是普遍的规律。

1930年，一位零售业富商，想捐款建造一所医学院，造福社会。当时的科学名流富莱斯纳告诉他，这些钱造一所医学院是不够的，而且纽约附近的医学院已经足够多。如果设立一个以数学为主的研究院，投资较少，而且美国正需要这样的基础性研究。这样，普林斯顿高等研究院便开始筹备。富莱斯纳到欧洲，请来爱因斯坦、外尔、冯·诺依曼三位顶尖的数理科学家，加上美国本土的三位数学家，强大的阵容一下子就把普林斯顿的学

术声誉推到云端。诺特在普林斯顿附近的一所女子学院任教，柯朗则在纽约大学工作。大批的数学难民从欧洲来到美国，造就了美国的数学辉煌。

冯·诺依曼来到普林斯顿高等研究院时只有 26 岁。他不仅在纯粹数学和应用数学上独树一帜，更伟大的创造是用数理逻辑方法设计数字电子计算机的方案。这一使用至今的科学精品，不仅是数学的骄傲，更是人类文明的里程碑。美国本土出生的数学家，也有杰出的成就，尤其是应用数学方面。例如，首创控制论的 N·维纳，提出信息论的 C·仙农，都是划时代的数学英雄。

差不多也在 1930 年代，另一个世界数学中心出现在莫斯科。大数学家欧拉曾在俄国工作多年，数学的积淀很深。1917 年“十月革命”胜利之后，国家经济一度十分困难。人们都在期待“面包会有的，牛奶也会有的”。可是，苏联的科学政策保证了科学研究的优先发展，数学家们可以经常出国访问，特别是到德国的格丁根大学。苏联的莫斯科大学有以鲁金为首的数学学派，起先以函数论为主，以后全面出击，泛函分析、变分学、概率论、集合论、偏微分方程等等学科，都有一流成果展现。

鲁金是沙俄时代留下来的数学家，在历次政治运动中倒也平安。据说斯大林曾经出面“保”过鲁金。鲁金招收了许多具有数学天才的年轻学者。其中，尤以 P·亚历山大罗夫和柯尔莫哥洛夫两人最为杰出，前者是世界拓扑学先驱，后者是 20 世纪少有的全能数学家。第二次世界大战期间，柯尔莫哥洛夫建立火炮自动跟踪技术，和维纳同时创立控制论。到了 1950 年代，

苏联数学可以和美国数学全面抗衡。

冷战时代苏美在军事上争霸，在数学上也处于彼此争雄的年代。不过，两国的数学家之间还是相当友好（难免有些小的摩擦），大家都统一在国际数学家联盟的数学大家庭中。

自从电子计算机问世以来，数学更趋向于应用。“一张纸、一支笔、一个脑袋”的研究方法，已被计算机的介入而打破。美国和苏联在军备竞赛中投入了大量的人力物力，都需要大量的数学投资，这就刺激和带动了数学科学的进步。美国和苏联的数学技术也长期在世界上继续领先。美国强大的经济力量，也支持了纯粹数学的研究计划。1991 年苏联解体和东欧政治变化之后，莫斯科数学中心的地位大为下降。一些优秀的苏联、东欧数学家相继到西方工作。最突出的例子是苏联数学大师 I·M·盖尔范德，以 80 岁高龄接受了美国罗格斯大学之聘，目前仍在美国数学界发挥作用。

苏美数学争雄结束之后，美国数学一枝独秀。但是数学中心也呈现多元化趋势。俄罗斯数学的威势仍存，莫斯科和圣彼得堡都有十分优秀的数学家在工作。圣彼得堡走出了佩雷尔曼，一举解决“庞加莱猜想”，却拒绝接受菲尔兹奖，堪称一代风范。以阿蒂亚为首的英国的牛顿数学研究所，法国的庞加莱数学研究所，德国的马克斯-普朗克数学研究所，日本京都大学的数学研究所，都是一定范围的数学研究中心。即使在美国，除了普林斯顿高等研究院之外，还有加州伯克利的美国数学科学研究所、明尼苏达的美国应用数学研究所，纽约大学的柯朗数学研究所也久负盛名。

目前国际数学大势是：美国继续领先，西欧紧随其后，俄国蓄势待发，日本正在迎头赶上。至于中国数学，目前还是未知数。一旦潜在的力量释放出来，北京也许是又一个国际数学中心。

近 50 年来，数学呈现出许多特点。

随着计算机技术的成熟和发展，数学从社会进步的幕后走到台前，进入数学的又一个黄金时期。计算机的硬软件设计基于数学，又推动数学。当数学模型能够实时控制生产和管理流程时，数学成为能够直接产生经济效益的“数学技术”。宏观的如数学控制论与航天技术，微观的如拓扑学扭结理论与基因的双螺旋结构；造福人类健康的 CT 扫描技术基于“Radon 变换理论”，随机微分方程用于金融股票价格的确定；艰深的数论公式成为保证国家安全的核心机密。时至今日，数据处理已经进入千家万户，成为人们日常生活中理财、决策时不可缺少的一部分。难怪“红楼梦的作者是谁”，也可以去问问数学家了。

数学和计算机技术联姻，并未放慢纯粹数学前进的脚步。费马猜想和庞加莱猜想的解决，是世纪之交数学科学的华采乐章。数学研究从线性问题跨到非线性问题，从交换情形发展到非交换情形。从低维空间问题推广到高维空间，却以 4 维空间为最大难点。当随机数学以确定性数学为工具进行研究的时候，复变函数中的毕卡定理用随机数学方法加以证明。新鲜事物穷出不穷，引无数数学英雄竞折腰。

一些哲学家和数学史家喜欢描述数学的三次危机。由罗素悖论触发的第三次数学危机至今并未完全渡过。然而，所谓的数学“危机”，不过是故作惊人之语。数学文明正在一日千里地

发展,依然绚丽多彩,无比灿烂。当 20 世纪的大数学家 D·希尔伯特、H·外尔、冯·诺依曼、柯尔莫哥洛夫等先后逝世之后,能够通晓当代全部数学的数学家已经远去。博大精深的当代数学,绝非本书编者能够了解于万一。我们只能远远瞭望,行注目礼,摘取其中的片段,和读者一起加以欣赏。若能有助于读者对当代数学文明有一个粗略的印象,使得数学融入大众文化,有助于青年学子追寻当代数学大家的创新足迹,本书的目的也就达到了。

中国数学正在与时俱进。随着国家实力的进一步增强,数学也正在一步步地走向世界。建立 21 世纪的数学大国,我们充满期待。

张奠宙　王善平

2009 年 8 月

目　录

1

诺贝尔奖中的数学

诺贝尔奖,是当代人类文明进步的标志之一。尽管并没有诺贝尔数学奖,但是数学成就依然在诺贝尔奖中扮演着重要角色。本章将介绍诺贝尔奖获得者工作中数学作用的一些典型事例。

1.1 诺贝尔、诺贝尔奖与数学

瑞典人阿尔弗雷德·诺贝尔(Alfred Bernhard Nobel, 1833—1896),被称为"现代炸药之父"。他发明了一种固体安全猛烈炸药以代替不安全的甘油液体炸药,还发明了用雷酸汞引爆炸药的装置——雷管。他一生中获得发明专利350多项,其中大部分与炸药有关。诺贝



图 1-1 诺贝尔

尔不仅是一位发明家，而且是一位成功的企业家。他在20多个国家中建立了工厂和实验室，大量制造炸药，既为战争提供了军火，也惠及采矿作业等民用需要。这使他积累了无数的财富。

虽然在大做军火生意，但诺贝尔骨子里仍然是一个世界和平主义者。他一生爱好科学、文学和艺术，写过诗、小说和剧本。在诺贝尔晚年的时候，曾有一家法文报纸误以为他已去世，遂发讣告，竟称“贩卖死亡之人已死亡”，指出他所发明的炸药杀死了许多人。这件事使诺贝尔深受震动，于是决心要用自己的财富为人类的文明和进步作贡献。

1. 诺贝尔的遗嘱

在去世的前一年，诺贝尔立下最后的遗嘱，规定身后全部遗产，除去一部分馈赠亲友外，剩下的全部转为一个证券投资基金。关于基金的作用，遗嘱中写道：

> 基金每年的利息将以奖金的形式，分给那些在过去一年里为人类作出最有益贡献的人。上述利息将被平分为5份，按如下方式分配：一份给在物理方面作出最重要发现或发明的人；一份给作出最重要的化学发现或改进的人；一份给在生理或医学领域作出最重要发现的人；一份给在文学领域创作出最杰出的理想主义作品之人；一份给曾为促进国家之间的友好，为废除或裁减常备军队以及为举行和平会议作出最重要贡献的人。物理和化学奖将由瑞典皇家科学院授予；生理学及医学奖由在斯德哥尔摩的卡罗琳医学院授予；文

学奖由在斯德哥尔摩的瑞典文学院授予；和平奖由挪威议会选出的一个五人委员会来授予。我的明确愿望是，在选择获奖者时，绝不考虑候选人的国籍；让最应得的人获奖，不管他是否是斯堪的纳维亚①人。

诺贝尔奖由此诞生。

2. 获得诺贝尔奖成为科学领域的最高荣誉

诺贝尔奖从 1901 年开始每年颁发，迄今已延续 100 多年，只是在第二次世界大战期间中止了 3 年(1940—1942)。诺贝尔奖一经问世，就赢得了全世界的尊崇。尤其是它在科学领域的奖项，包括物理奖、化学奖、生理学及医学奖，已成为科学家梦寐以求的最高学术荣誉。



图 1-2　诺贝尔奖章

诺贝尔奖受人推崇的主要原因有两个：其一是它的奖金极为丰厚。最初的每份奖额约 3 万多美元；由于基金管理机构投资有方，使得奖额逐年增长；到 2005 年，每份已达到约 130 万美元。如此丰厚的奖金足以明显改善科学家的生活和工作条件。

其二因为它是第一个不考虑国籍、种族、性别或意识形态，完全以学术价值为评判标准的世界性科学大奖。负责推荐和挑选获奖者的人都是有关领域的知名专家；而评奖委员会的工作

---

①　斯堪的纳维亚系指北欧半岛，主要包括瑞典和挪威两个国家，这两个国家在 1814—1905 年期间曾形成以瑞典为主导的联盟，当时规定瑞典国王也是挪威的国王。

程序则保证了结果的公正性和权威性。科学家因获得诺贝尔奖为荣，反过来，诺贝尔奖也因为有爱因斯坦、居里夫人等伟大科学人物而著称。可以毫不夸张地说，诺贝尔奖获得者的工作代表了当代人类最先进的科学水平和成就。拥有多少名获得过诺贝尔奖的科学家，则成为衡量一个国家科技实力的重要尺度。100 多年来获得诺贝尔奖的科学工作，已经成为人类文明的一个重要组成部分。

3. 没有诺贝尔数学奖

数学是对于人类的文明发展和社会进步最有影响的一门科学，但它却没有被纳入诺贝尔奖中，其中原因引起不少探究。一种广泛流传的说法是，诺贝尔与同为瑞典人的著名数学家米塔-列夫勒(Magnus Gustaf Mittag-Leffler，1846—1927)交恶。为防止米塔-列夫勒获奖，诺贝尔故意不设数学奖项。这种说法显然与诺贝尔在其遗嘱中所体现的摒弃狭隘意识，以人类进步和福祉为怀的博大胸襟不符。

另一种较为合理的解释是，诺贝尔对数学不是很了解，因而可能认为数学研究的东西太抽象，对于人类社会较少有直接的贡献，所以在设立奖项时没有想到数学。

其实，虽然自 19 世纪以后，数学逐步发展成为一门高度抽象的科学，但它始终与现实世界保持密切联系。数学是人类洞察事物奥秘、认识世界的强有力的思维工具。尤其是进入 20 世纪以后，几乎任何一门科学的发展都离不开数学的帮助。

虽然诺贝尔奖中没有专门的数学奖项，但是数学在很多获

奖工作中起了关键作用，甚至有不少获奖者本身就是数学家。

1968 年，瑞典中央银行增设了诺贝尔经济学奖，该奖项每年与其他诺贝尔奖项同时颁发。迄今为止，几乎所有的诺贝尔经济学奖的获奖工作都是数学在经济学领域的应用，而且大部分获奖者是数学家或具有很高数学素养的经济学家。

诺贝尔奖没有覆盖的重要科学领域包括数学、地球科学、生物科学(特别是关于生态学和进化论)和天文学。1980 年由人工肾脏发明者霍尔格·克拉福德和他的妻子安娜-格蕾塔·克拉福德设立了克拉福德奖，由瑞典皇家科学院管理。现在奖金为 50 万美元，接近诺贝尔奖的奖金。由于每年只颁发一个奖项，使得每个学科六七年才轮到一次，影响力相对较小。

2001 年 8 月，挪威王国政府宣布，在阿贝尔诞生 200 周年之际，设立面向国际的“阿贝尔数学奖”。该奖仿效“诺贝尔奖”，每年颁发一次，奖金额为 87.5 万美元，是目前国际数学奖中奖金额最大的奖项，与诺贝尔奖 100 万美元左右的奖金差不多。挪威和瑞典曾经结盟，关系密切，因此挪威政府创立该奖可以看做是弥补诺贝尔奖中没有数学奖的遗憾。

为了弥补诺贝尔奖中不包括数学的遗憾，由国际数学联盟(International Mathematical Union，IMU)领导的国际数学家大会(International Congress of Mathematicians，ICM)从 1936 年起，每四年颁发一次菲尔兹奖章，菲尔兹奖章的学术荣誉相当于诺贝尔奖，所以经常被称为“数学诺贝尔奖”，不过它的奖金额比诺贝尔奖少得多。详细介绍见本书第 5 章。

1.2 重建人体内部的三维图像

——计算机X射线断层成像(CT)的数学理论

到医院做CT检查,现在已经成为人们的常识。这是计算机技术造福人类的一个重要事件。但是,它的核心思想,是基于一项称为"拉东变换"的数学工作。

1. 从X光透视说起

德国物理学家伦琴(Wilhelm Conrad Röntgen, 1845—1923)在1895年宣布发现了X射线,他因此获得1901年首届诺贝尔物理学奖。伦琴也许不曾想到,他的发现很快在医学诊断领域得到了广泛的应用。因为X射线具有强大的穿透能力,能够轻易地通过人体。这使得医生无需施用外科手术,就能透视人体,从而作出准确诊断。

当X射线通过人体时,对于体内的不同组织,如肌肉、血管、骨骼、脏腑等,有不同的穿透率;体内病变的组织,如发炎或肿瘤,它们的X射线穿透率也与正常组织不同。所以如果将人体置于X射线源与感应胶片之间,就能在胶片上留下体内组织的X射线投影像,医生则可以根据影像来诊断病情。这就是传统的X射线成像仪的工作原理。

如图1-3所示,从X射线源发出X光穿过人体,使后面的胶片感光,留下人体的X射线投影像。医生可以根据影像,对病情作准确判断。



图1-3　X射线透视人体的原理图

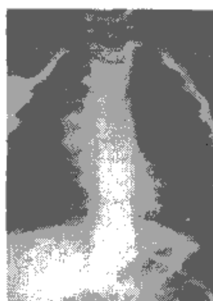


图1-4　X射线人体胸部透视图像

然而，由传统X射线成像仪所形成的人体内部纵向面的投影像，只包含了体内组织的二维结构信息，它无法提供体内横截面(断层)上组织的情况。所以，虽然传统X射线成像仪对于诊断骨折或肺部感染之类的病情有很大帮助，但对于诊断脑部疾病或内脏肿瘤之类的疑难杂症却无能为力。

在很多诊疗场合，医生非常需要获得病人体内组织的断层结构信息，但只有切开身体，才能观察到体内断层，而这将不可避免地伤害病人，甚至危及生命。

1972年，在英国出现了一种神奇装置，被叫做“计算机辅助X射线断层成像仪”(computer assisted tomography，简称CAT或CT)；它能够在不损伤病人的情况下，提供人体从头到脚各部位的断层X射线图像。利用CT，医生可以轻而易举地观察到人体内部哪怕是微小的病变和病灶分布，能够及早采取正确的治疗措施，从而拯救了无数患者的生命。



图1-5　病人在接受CT诊断

1979 年 10 月 11 日，诺贝尔的诞辰日，位于瑞典首都斯德哥尔摩的卡罗琳医学院宣布，当年的诺贝尔医学奖授予美国人柯马克(Allan MacLeod Cormack，1924—1998)和英国人豪斯菲尔德(Godfrey Newbold Hounsfield，1919—2004)，以表彰他们“发明了计算机辅助 X 射线断层成像技术”。卡罗琳医学院的葛雷茨(Torgny Greitz)教授在授奖发言中说：“今年诺贝尔生理学及医学奖的两位获奖者都不是医学专家，然而他们在医学领域掀起了一场革命……他们发明的计算机辅助 X 射线断层成像技术，使医学如同进入了太空时代。”“没有什么医学成就能够像 CT 技术那样，立即被广泛接受并得到毫无保留的热烈欢迎。”“柯马克和豪斯菲尔德开创了医学诊断的新时代……(他们的工作)正符合诺贝尔在其遗嘱中有关‘为人类作出最有益贡献’的规定，没有几位诺贝尔生理学及医学奖的获得者能够达到像他们那样的符合程度。”

2. CT 成像基于数学原理

CT 是如何做到在不损伤病人的情况下获得病人体内横断层的图像的？原来，它借助于一种叫做“拉东变换”的数学理论。

如前所述，人体内部不同的组织具有不同的 X 射线衰减率(穿透率)。所以，如果能够知道人体内 X 射线衰减率的分布，就能够重建体内组织的图像了。这正是 CT 所要做的。

如图 1-6 所示，一束 X 射线从一定点 A 穿过人体，到达 P 点。由于在途中经受不同物质的吸收，所以在 P 点接收到的 X 射线的强度较在 A 点出发时有了一定的衰减，其衰减程度与

AP 间物质的平均 X 射线衰减率有关。从而,通过比较和计算,可以求出从 A 点到 P 点的平均 X 射线衰减率。令 X 射线源沿着圆周从 A 点移动到 B 点,发射的 X 射线将从 B 点穿过人体达到 Q 点。同样道理,可以计算求出从 B 点到 Q 点的平均 X 射线衰减率。于是,令 X 射线源沿圆周移动一圈,以不同的角度分别发射 X 射线穿透人体,就得到了无数的不同角度直线上的平均 X 射线衰减率。

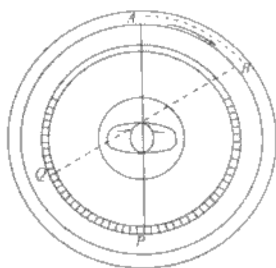


图 1-6　CT 工作原理图



图 1-7　CT 颅脑摄影像

1917 年,奥地利数学家拉东(Johann Radon,1887—1956)发表了一篇论文,其中提出,对于一个定义在一定区域上的函数 f,如何从该函数在以不同角度穿过该区域的直线上的积分值,来求得其分布解的变换方法。这个积分就被称为 f 的拉东变换,其表达式为

$$R[f](\alpha,s)=\int_{-\infty}^{+\infty}f(x(t),y(t))\mathrm{d}t,$$

f 函数的分布解可通过对 R 进行逆变换得到。

于是,如果把人体中不同组织的 X 射线吸收率当作一个函数,把通过以上方法求出的不同直线上 X 射线平均衰减率看做是函数在该直线上的积分值,那么利用拉东变换方法,我们就得

到了人体内部的 X 射线分布解，从而能够重建体内的图像。这就是 CT 的工作原理。当然，拉东并没有想到他的成果会在 60 年后被用于医学。

3. 数学和医学的结合

1963 年 CT 理论奠基者柯马克发表题名为“函数的直线积分表示及其放射学应用”的开创性论文，从而奠定了 CT 的理论基础，实现了数学和医学的一次完美结合。

柯马克出生于南非的约翰内斯堡，父亲是电信工程师，母亲是教师。柯马克在南非开普敦大学攻读电气工程专业，在那里打下了扎实的数学和物理学基础，获得学士和硕士学位。1956 年，柯马克移居美国，并在波士顿的 Tuft 大学任物理学教授，直至 1995 年退休。



图 1-8 柯马克

在 1955 年的一段时间，作为物理学讲师的柯马克接受到一项任务，要为一家南非医院的放射科监测肿瘤患者接受放射性同位素治疗的剂量。接受治疗的患者体内的同位素剂量及其分布应该受到严格的控制：如果同位素剂量太小，将达不到理想的疗效；剂量太大，则会危害患者的健康。同时，同位素的浓度应在肿瘤组织内较高，在健康组织内尽可能低。柯马克于是想，是否可以通过体外测量同位素发出的射线，来确定其在体内的浓度分布，以帮助医师确定最佳治疗方法？他很快发现这其实是一个数学问题，而且发现，若解决了这一问题可以在放射医学中

有种种应用。他终于在 1963 年发表题名为“函数的直线积分表示及其放射学应用”的开创性论文。这是 CT 成像技术的理论基础，数学应用的又一次重大突破。

顺便提一下，柯马克研究 X 射线成像问题纯粹出于业余爱好，既没有获得任何的经费资助，也不算他作为大学物理学教师的工作量。

柯马克的成果一开始没有引起人们多少注意，因为要重建能够用于临床诊断的高质量的人体图像必须进行大量的数值计算，靠手工来做显然不行，当时水平的计算机也帮不了多少忙。

1972 年，直到计算机技术有了长足的发展之后，才由英国电气音乐有限公司(EMI)的计算机工程师豪斯菲尔德造出了第一台可用于临床的高精度 CT，即计算机辅助 X 射线断层成像仪。



图 1-9　豪斯菲尔德

豪斯菲尔德出生于英国诺丁汉郡农村，毕业于一家电气工程专科学院，第二次世界大战中在皇家空军服役，他没有大学学历。豪斯菲尔德因为发明了 CT，于 1981 年被授予爵士称号。

未来之舟

作为 CT 技术的数学理论基础的拉东变换有着广泛的应用。例如，当用 γ 射线代替 X 射线时，就得到了 γ 射线的 CT；如果使用质子或正电子，就会相应得到质子或正电子的 CT。这些 CT 图像有着不同于 X 射线图像的意义。比如说，正电子 CT(PET)能够提供病人体内新陈代谢水平的分布图像。此外，拉东变换还可以用于其他领域，如测量海水温度分布、观察天体运动，等等。

磁共振成像(magnetic resonance imaging，简称 MRI)被称为是 CT 之

后医学影像技术的又一大进步。其原理是让人体内部组织的氢原子核在外界恒定磁场和梯度磁场的作用下产生磁共振并激发出无线电信号，然后利用傅里叶变换(Fourier transformation)和拉东变换等数学工具，把接收到的电信号转为人体图像。与CT相比，MRI能够提供更多的关于人体内部组织的功能和代谢等信息，并且不会对人体形成放射性伤害。2003年的诺贝尔医学奖分别授予了美国物理学家保罗·劳特伯尔(Paul C. Lauterbur, 1929—2007)和英国物理学家彼得·曼斯菲尔(Peter Mansfield, 1933—)，以表彰他们发现了磁共振成像的原理并且找到了重建图像的数学方法。

另据报道，CT和MRI技术正开始广泛用于木材的无破坏内部检测，它们将大大提高木材的使用效率并降低生产成本。

1.3 X射线直接测定晶体结构的数学方法

两个非名牌大学数学系的毕业生，为测定各种物质的晶体结构提供了一种数学方法。于是，一个普通的大学生可以测知当年获得诺贝尔化学奖的大家才能得到的晶体结构信息。数学，再次体现其王者风范。

1. 关于晶体的几何结构

中学的化学知识告诉我们，晶体是物质存在的一种基本形式，其特征是，具有规则的形状、固定熔点和各向异性的光学性质。从几何的角度来看，晶体就是物质的质点(离子、原子或分子)由于彼此间的作用力而形成规则的空间结构。根据质点和作用力的不同，可以把晶体分为离子晶体、金属晶体、原子晶体和分子晶体这四大类。晶体中的质点相互连接而形成空间点阵。晶体的最小构成单位是晶胞，其形状一般为平行六面体。

相同的晶胞聚列而成各种晶体。

许多金属和非金属的单质、无机和有机化合物都能够以晶体的形式存在，如氯化钠(食盐)(图 1-10)、石墨、金刚石、钢铁、合金、塑料，各种药物，包括抗生素和维生素，以及作为生命基本结构的蛋白质与核酸，等等。另外，液晶是一种具有液体形态的有机分子晶体，因具有独特的光电效应性质而成为理想的信息显示材料。目前，液晶显示已广泛用于电视机和计算机。

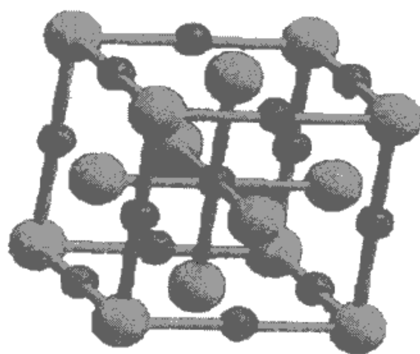


图 1-10　氯化钠(食盐)结构图

无论是作为工业材料、药物，还是作为生命物质，晶体的种种性质和功能，以及形成晶体的方式，都取决于其几何结构。因此，研究晶体的一项基本任务就是设法测定它的结构，从而能够彻底了解它的性质，掌握它的作用，并且帮助找到有效的生产或合成方法。

然而，构成晶体点阵的质点间距极小，它比人的头发丝直径的数十万分之一还要小。人们究竟用了什么方法，才能测定晶体的结构呢？原来是借助于 X 射线这一奇妙的工具。

2. 青霉素晶体几何结构的获得

1912 年，德国科学家劳厄(Max von Laue，1879—1960)发现 X 射线在穿过晶体时会发生衍射。这一发现在科学界引起轰动，因为它一下子解决了两个悬而未决的大问题：第一，它证实了 X 射线就是电磁波，即也是一种光线，只是波长极短，因而人眼看不见；第二，它揭示了晶体的微观结构。因为光线只有在绕过间隙与波长相近的物体时，才会产生衍射，所以这表明 X 射线的波长与晶体点阵中相邻质点的间隔(即键长)具有相同的数量级：$10^{-11}\sim10^{-9}$ 米。劳厄还给出了计算晶体点阵衍射的数学公式。1914 年，劳厄因他的成就而获得了诺贝尔物理学奖。

在获悉劳厄的工作之后，英国科学家布拉格父子(William Henry Bragg，1862—1942；William Lawrence Bragg，1890—1971)立即认识到，X 射线是窥探晶体结构的理想工具。于是开始把 X 射线对准了不同的晶体，很快就获得了氯化钠(食盐)、氯化钾、氟化锂、二硫化铁、二氟化钙、钻石等一大类碱金属卤化物和单质晶体的结构信息。他们改进劳厄公式，推出了准确描述 X 射线波长、晶体点阵间距与衍射角度之间关系的简明公式。布拉格父子因此同获 1915 年诺贝尔物理学奖，成为科学史上一段佳话。

劳厄和布拉格父子的工作开创了 X 射线晶体学。然而，用 X 射线测定结构较复杂的晶体，特别是那些在生物学和生理学上有重要意义的有机分子晶体，这绝非易事。为了测定一些晶体结构，科学家需要付出艰巨的劳动。

在小布拉格的支持和帮助下，英国剑桥大学的科学家佩鲁茨(Max Ferdinand Perutz，1914—2002)与肯德鲁(John Cowdery Kendrew，1917—1997)花费了 16 年，于 1953 年最终测定了血红球蛋白的结构。球蛋白是分子结构最简单的一种蛋白晶体(图 1-11)。他们因此获得了 1962 年诺贝尔化学奖。

英国牛津大学的女科学家霍奇金(Dorothy Crowfoot Hodgkin，1910—1994)花了 4 年时间，于 1946 年测定了青霉素的结构(图 1-12)；使得这种曾经比黄金还贵的威力强大的抗生素能够以较低成本大规模生产，还使得科学家能够发现和培养结构相近、功能多样的其他抗生素，从而拯救了无数病人的生命。霍奇金又从 1948 年开始测定维生素 B_{12} 的结构，经过 8 年不懈的努力，于 1956 年获得成功。霍奇金由于她的卓越的工作而获得 1964 年的诺贝尔化学奖。

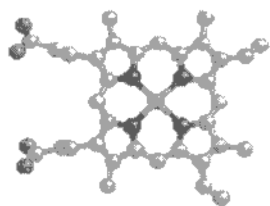


图 1-11　血红球蛋白的分子结构图

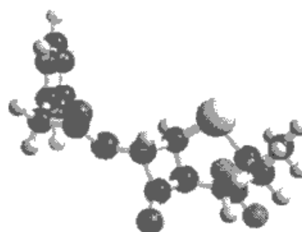


图 1-12　青霉素的分子结构图

霍奇金、佩鲁茨和肯德鲁所测量那些晶体的结构其实不十分复杂，但她/他们为什么要花费那么多的年月才完成测量，并能获得最高的科学奖赏？原来，以当时科学家的认识水平，在 X 射线晶体衍射图中，包含晶体结构的信息不完全。因此，为了测定晶体的结构，不得不大量采用其他的物理化学方法，如根据原

子的物理性质推断它们的连接方式，将待测物质分解或与其他物质组成新的化合物以获得关于结构的补充信息，等等。每测量一种晶体，就好像攀爬一座高耸的山峰，需要科学家集中全部的才智、勇气和毅力，经过多少次尝试和失败，才有可能获得成功。所以霍奇金和佩鲁茨等人获得诺贝尔奖当属实至名归。

然后，美国数学家豪普曼（Herbert A. Hauptman，1917—）与物理化学家卡勒（Jerome Karle，1918—）联袂登场了。他们使事情一下子变得简单起来。

3. 高深的数学介入晶体几何结构的测定

在美国海军研究实验室工作的豪普曼与卡勒，从 1947 年起开始合作研究 X 射线晶体衍射。为了更准确地描述问题，他们从分析晶体的量子力学模型着手。

量子力学是一种能够精确描述微观物质状态和行为的现代物理学理论，由丹麦人玻尔和德国人海森堡等一批物理学家在 20 世纪 20 年代创立。根据量子力学，电子按一定的概率分布出现在原子核周围，形成电子云。而晶体内连接相邻原子的化学键则由有关的电子概率分布函数决定。由于晶体是由完全相同的平行六面体晶胞排列而成的，所以那些电子概率分布函数都是三维的周期函数，因而可以用三维傅里叶级数来表示。

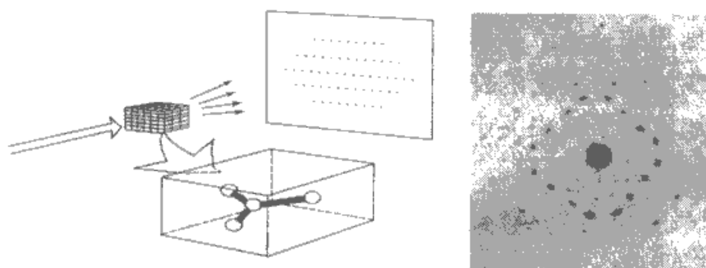
傅里叶级数理论　19 世纪法国数学家傅里叶（Jean Baptiste Joseph Fourier，1768—1830）为研究热传导问题而创立。其核心思想是用正弦和余弦的三角函数的级数来表示所有的周期函数，即对于满足一定条件的周期函数 $f(x)$，总可以表示成

$$f(x) = \sum_{n=0}^{\infty}(a_n \sin n\omega x + b_n \cos n\omega x)。$$

晶体内电子概率分布函数的每项傅里叶级数的系数被称为结构因子，它们是复数。显然，晶体的结构由这些结构因子唯一确定。

当 X 射线通过晶体时，产生衍射，并在前方的感光胶片上形成衍射图像(图 1-13)。

在一般情况下，一个晶体的 X 射线衍射图像中可以出现数千条甚至上万条衍射条纹。可以证明，这些衍射条纹完全确定了晶体结构因子的“大小”(即这些复数的模)，但不能确定它们的“相位”(即复数的实虚部之比)。因此，当时的科学家相信，由于 X 射线衍射图中缺失了晶体结构因子的相位信息，所以必须使用其他的辅助方法，才能完全测定晶体的结构。



(a)X 射线晶体衍射形成示意图　　(b)产生的衍射图像照片

图 1-13

然而，豪普曼和卡勒经过多年的探索，发现情况并非如此。利用傅里叶级数的变换性质，并根据电子密度函数总是非负的、在原子的位置上取最大值等条件，可以把晶体的结构因子表示成晶体内原子的位置向量函数。由于一个待测晶体的晶胞内通

常有数十个或上百个原子，一个三维位置向量有三个分量，所以这些函数一般含有二三百个未知数。而X射线每一条衍射条纹就可以决定一个关于这些位置向量的方程，并且至少有数千条这样的衍射条纹。所以得到了关于数百个变量的数千个方程。由于方程个数远远多于未知量的个数，这说明在X射线的衍射图中包含了晶体内原子位置的完全信息，因而也包含了晶体结构的完整信息，从而推翻了当时的流行论断。

当然，由于这些方程都是非线性方程，所以求解它们十分困难。豪普曼和卡勒运用概率统计、群论和代数学的知识，并借助于计算机，终于建立起求解这些方程的一整套方法。人们称这套方法为“直接法”，因为它无需借助其他物理或化学的辅助方法，可以通过X射线的衍射直接测定晶体的结构。有了这套方法，如今一个普通的大学生就能轻松算出霍奇金和佩鲁茨等人当年花费九牛二虎之力才得到的结果。



图1-14　豪普曼



图1-15　卡勒

1985年，瑞典皇家科学院宣布，这一年的诺贝尔化学奖授予豪普曼和卡勒，“以表彰他们因创立测定晶体结构的直接法而取得的杰出成就”。

瑞典皇家科学院的林奎斯特(Ingvar Lindqvist)教授在授奖

发言中指出：

> 此次诺贝尔化学奖授予了数学家豪普曼和物理学家卡勒……由于他们的想象力和创造性，使得人们测定通常晶体结构时不再需要想象力和创造性。
>
> X 射线测定晶体结构的直接法为化学家更快更深入地研究分子结构以及化学反应提供了有效的工具。

4. 大学数学系的毕业生

豪普曼 1917 年 2 月 14 日出生于美国的纽约市。他从小就喜欢数学和自然科学。1937 年纽约城市学院数学专业毕业，获学士学位；1939 年获哥伦比亚大学数学专业硕士学位。1940 年结婚，并在美国统计局任职。第二次世界大战的战火燃烧到美国后，豪普曼应征入伍，曾任海军少尉，负责天气预报；又去菲律宾，任消防官员；最后到美国空军，担任雷达教员。战争结束后，豪普曼于 1947 年进入美国海军研究实验室，在那里遇到了卡勒，于是两人开始了长期的 X 射线晶体衍射研究的合作。他们的研究因与当时“X 射线衍射中不包含晶体结构完全信息”的流行看法不符，因此引起不少争议，不断受到怀疑和反对，许多人认为他们在浪费时间。但他们不为所动，坚持研究，终获成功。

豪普曼于 1955 年获马里兰大学数学专业的博士学位。当时他一边做研究，一边读博士，还要照看 3 岁的女儿，而且把这三件事都做得很出色。1970 年，豪普曼离开工作了 20 多年的海军研究实验室，来到布法罗医学基金会，任晶体组研究主任。

豪普曼并非毕业于名牌大学，但由于他永不放弃的精神和

勤奋的工作态度,终于作出了卓越的科学贡献。

未来之舟

X射线晶体学是确定生物大分子,尤其是蛋白质和核酸(如DNA、RNA)构象的主要方法。被认为包含了生命全部遗传信息的DNA分子的双螺旋结构就是通过晶体学实验数据发现的。目前,全世界的生物学家正在合作建设网上蛋白质数据库,将已测明结构的蛋白质和其他生物大分子的数据信息上传,供人们免费查询。截至2007年5月,该数据库已包含了43 000多种蛋白质和核酸等分子的结构信息,其中85%以上是通过X射线衍射方法测定的。

1.4 对称、守恒、规范场与群论

由于在20世纪的头四分之一世纪里,革命性的狭义相对论、广义相对论和量子理论相继问世,使得人类对于物理世界的构成和运动,有了相当深刻和精准的认识。我们现在确信,我们周围所有的物质都是由原子构成,原子由电子和原子核构成,而原子核则由带正电的质子和不带电的中子构成。物质所有的运动和变化都是由于4种基本力的作用,那就是支配天体运动的万有引力,决定物质的通常物理和化学性质并能使电气电子设备工作的电磁力,把质子和中子牢牢地绑在原子核中的强力,以及参与原子核衰变的弱力。理论物理学家目前所面临的中心任务,就是要在数学的框架下,探求能够描述这四种基本作用力的统一的理论。创立了相对论的大物理学家爱因斯坦(Albert Einstein,1879—1955)在他的后半生中致力于发展统一场论,可惜没有成功。目前,最有希望统一宇宙基本作用力的是规范场理论。

1. 宇称不守恒是对称破缺

1957 年，杨振宁（1922—）与李政道（1926—）因提出在弱力作用中宇称不守恒的理论而荣获该年的诺贝尔物理学奖。

宇称是表征粒子或粒子组成的系统在空间反射下变换性质的物理量。在空间反射变换下，粒子的场量只改变一个相因子，这个相因子就称为该粒子的宇称。我们也可以简单地理解为，宇称就是粒子照镜子时，镜子里的影像。以前人们根据物理界公认的对称性认为，宇称一定是守恒的。但是，这一金科玉律被打破，出现了“对称破缺”。

弱力的对称-守恒关系，竟然在宇称（即左右对称或镜像对称）情况下不成立！

这个道理其实很简单。对称性反映不同物质形态在运动中的共性，而对称性的破坏又使得它们显示出各自的个性。如同建筑和图案一样，只有对称而没有它的破缺，看上去虽然很规则，却会显得单调和呆板。只有基本上对称而又不完全对称的建筑和图案才会显示特别的美感。大自然正是这样的建筑师。当大自然构造像 DNA 这样的大分子时，总是遵循复制的原则，将分子按照对称的螺旋结构连接在一起，而构成螺旋形结构的空间排列。但是在复制过程中，对精确对称性的细微的偏离就会在大分子单位的排列次序上产生新的可能性，从而使得那些更便于复制的样式更快地发展，形成了发育的过程。因此，对称性的破坏是事物不断发展进化，变得丰富多彩的原因。

杨振宁和李政道完成了理论上的推想之后，请求实验物理

学家吴健雄博士进行实验证实。随后,吴健雄博士与华盛顿的美国国家标准局的阿贝尔博士商讨合作这一实验的可能性,实际工作在3个月后开始。她在极低温度(绝对零度以上0.01℃)的磁场中,观测钴60衰变为镍60,及电子和反微子的弱交换作用,果然电子及反微子均不遵守宇称守恒原理。

实验成功了,吴博士证明了杨振宁和李政道的理论,推翻了物理学上屹立不移三十年之久的宇称守恒定律。美国作家李·伊得逊说:吴健雄博士经过了不知多少次艰辛而复杂的实验,方使杨、李二位在理论上的突破,获得了实验上的证明。吴健雄在实验中发现了电子倾向于左手旋的现象,不仅改变了物理科学中"宇称守恒"的基本信念,同时也影响到化学、生物、天文和心理学的发展。虽然吴健雄博士没有得到诺贝尔奖,但她所从事工作的重要性并不因此而降低。

物质结构是用对称语言写成的。对称守恒和对称破缺,都是对称性的体现。

杨振宁回忆他的大学生活时说,对我后来的工作有决定影响的一个领域叫做对称原理。在"对称和物理学"一文的最后,他写道:"在理解物理世界的过程中,21世纪会目睹对称概念的新方面吗?我的回答是,十分可能。"杨振宁和米尔斯在1954年建立的非交换规范场论,更使在对称性研究上取得了更重要的突破。

2. 电磁场和一维李群 $U(1)$

1905年,爱因斯坦根据宇宙中没有绝对静止的物理坐标系,

所有相对匀速运动的物理坐标系都是等效的假设，创立了狭义相对论。从中得出“物体质量随运动速度增加而增大”，“质量和能量可相互转换”，以及“光速是极限速度”等惊人结论，后来竟都得到了实验的证实。

1913年，爱因斯坦又根据所有相对加速运动的物理坐标系也都是等效的假设，创立了广义相对论。又给出“引力使空间弯曲”的不可思议断言，同样得到了实验印证。爱因斯坦曾因分析广义相对论的“弯曲空间”中物理现象遇到困难，而求助于同学兼好友的数学家格罗斯曼(Marcel Grossmann，1878—1936)。后者告诉他，60年前德国数学家黎曼已创立了一种几何学，它正是研究弯曲空间的理想工具(详见本书2.1节)。



图1-16 爱因斯坦

1921年，爱因斯坦荣获了诺贝尔物理学奖，但不是因为创立了相对论，而是由于“发现了光电效应的规律”。因为相对论的思想惊世骇俗，当时负责挑选诺贝尔物理学奖候选人的瑞典皇家科学院对于它的正确性还存有疑虑。

相对论中关于运动物理坐标系“等效性”的假设可以用数学语言描述为，物理规律在一些特定的时-空坐标“运动子群”的变换下保持不变；特别地，牛顿运动方程和麦克斯韦电磁方程之类的数学公式，应该在一些随时间变化的坐标变换下保持形式不变。这其实反映了物理规律在时-空中的一种对称性，这种对称的思想在爱因斯坦以后大大发展，成为现代理论物理研究的核

心内容。而现代数学中的“群论”,则是研究对称性的理想工具。

群论 由19世纪法国天才数学家伽罗瓦(Évariste Galois,1811—1832)在19岁时创立。他为了解决代数方程的根式可解性问题,而研究方程根之间的置换。如2次方程 $x^2+1=0$ 有两个根 $\theta_1=\sqrt{-1}$,$\theta_2=-\sqrt{-1}$,则有两个置换:

$$\tau_1:\theta_1\rightarrow\theta_1,\theta_2\rightarrow\theta_2 \text{ 和 } \tau_2:\theta_1\rightarrow\theta_2,\theta_2\rightarrow\theta_1$$

一个方程的所有根置换构成了一个群,即它满足群的三个定义条件:(1)存在一个恒等置换(称为群的单位元,以上例子中的 τ_1 就是单位元);(2)两个置换的复合(称为群的乘法)也是置换;(3)对于每个置换都存在另一个置换,使得这两个置换的复合正好是恒等置换(即群中的每个元素都有可逆元)。

伽罗瓦证明了一个代数方程有根式解当且仅当它的根置换群是可解群。4次及以下方程的根置换群都是可解群,所以都有根式解。5次方程中有的置换群不可解,所以5次方程一般没有根式解。

容易证明,所有的时-空坐标的平移、旋转和镜像等变换满足群的定义条件,所以它们构成了时-空坐标变换群中的一个子群,即运动群。而爱因斯坦的相对论假设中所涉及的坐标运动则属于运动群中的子群。

德国数学家外尔(Hermann Weyl,1885—1955)受到广义相对论的“弯曲空间”和“物理规律在时-空运动子群的作用下不变”的假设启发,试图把电磁场也归结为某种时-空变换下的物理对称性。不过,他不是像相对论那样研究整体时-空中的运动变换,而是研究局部时-空中的“尺度变换”。

外尔在 1918 年提出，物理空间中相邻“无穷小”①的两个点上的“尺度”应有所不同。为了保持当坐标从其中一点平移到另一点时物理规律的不变性，需要引进一个向量数，被称为“尺度因子”。外尔称这种物理规律的对称性为“规范不变性”，其中“规范”就是指尺度。他认为这里的尺度因子就是刻画电磁场的电动势。以后的研究表明，为保持物理规律的“规范不变性”，应该引入“相位因子”而不是“尺度因子”，两者之间正好相差一个虚单位因子 $\sqrt{-1}$。也就是说，相位因子正好是电磁场的电动势乘上 $\sqrt{-1}$。就这样，外尔成功地把电磁场归结为物理规律的“规范不变”性质。



图 1-17　外尔

后来人们才发现，外尔引入的“相位因子”其实是 $U(1)$“李群”。李群就是一种带有可微几何结构的群，由挪威数学家李(Marius Sophus Lie，1842—1899)率先研究。李群在现代物理学中有重要应用。运动群也属于李群。$U(1)$群，同构于圆群，即可以用复平面上的单位圆来表示：$\{e^{i\theta} \mid \theta$ 为实数$\}$。其上定义的群运算是

$$e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$$

注意这个运算是可以交换的。

外尔是把群论，特别是李群，用于物理学研究的先驱。他在 1928 年出版的《群论与量子力学》是数学和物理学的经典名著。

① 这属于高等数学中的“微分”概念。

不过，他当时还没有注意到，他所创立的规范场和所钟爱的李群之间有什么联系。

3. 杨振宁-米尔斯：同位旋守恒和非交换群 *SU*(2)

事实上，人们更多的是从以下方面来理解“对称性”对于物理学的重要意义：那就是“对称性”与各种物理守恒定律之间的相互对应关系。这种深刻关系是由德国著名的女数学家诺特(Emmy Amalie Noether，1882—1935)在1918年发现的，因而被称为“诺特定理”。诺特定理的大意为：任何在一连续变换群作用下保持不变的物理规律，都对应一种守恒定律，反之亦然。比如说，物理的时间平移不变性对应于著名的能量守恒定律；空间平移不变性对应于动量守恒定律；空间旋转不变性对应于角动量守恒定理。又如，我们已知道，电磁场是“规范不变性”的产物，它所对应的则是电荷守恒定律。



图 1-18　诺特



图 1-19　杨振宁

在20世纪30年代，物理学家发现质子和中子除了一个带电另一个不带电之外，在其他方面几乎完全一样；特别是，如果不考虑电磁场的影响，在强力作用中，两者无法区分。为了描述

这种现象，物理学家引进了同位旋量子数的概念：质子和中子只是处于不同的同位旋状态的同一种粒子。

同位旋量子数在强力作用下守恒，根据诺特定理，它应该对应于一种物理对称性。那么，究竟是怎样形式的对称呢？

1954 年，正在美国布鲁克海文国家实验室访问的中国年轻物理学家杨振宁与美国人米尔斯（Robert L. Mills，1927—1999）合作发表了题名为“同位旋守恒和同位旋规范不变性”的论文，指出同位旋守恒与电荷守恒类似，也对应于一种规范不变性。上面提到，外尔用李群$U(1)$刻画电磁场的规范不变性。同位旋守恒所对应的不变性，则由 $SU(2)$李群变换所决定。这是一个由行列式恒为 1 的二阶矩阵所描述的群。由于矩阵乘法一般是不可交换的，在数学上称为非阿贝尔群。从交换的 $U(1)$李群，跨越到非交换的 $SU(2)$李群，情况要复杂得多。

文章推广了麦克斯韦电磁场方程，得到著名的杨-米尔斯规范场方程。于是，杨振宁和米尔斯首创了“非交换规范场的理论”。

杨振宁的父亲杨武之（1886—1973）长期担任清华大学的数学教授，研究数论，是他发现了中国数学奇才华罗庚（1910—1985）。杨振宁早在高中时代，就从父亲那里了解了有关群论的基本知识，领略到“群论无与伦比的美妙和力量”。后于 1938—1942 年在西南联大物理系读本科，1942—1944 年留校读硕士研究生，1946 年赴美国芝加哥大学学习，1948 年获博士学位。在大学读书期间，杨振宁系统学习并掌握了群论在物理学中的种种应用。特别在读研究生阶段，开始研究外尔的有关电磁规范

场的工作，对于“规范不变性决定了全部电磁相互作用这个事实”留下了极其深刻的印象。于是着手要把这种观念推广到同位旋的作用上去。经过数次失败后，终于与米尔斯合作取得了成功。米尔斯后来回忆道①：“1954年我在布鲁克海文做博士后，与杨振宁在同一间办公室。杨振宁当时已在许多场合中表现出乐于帮助青年物理学者。他把推广规范不变的想法告诉我，我们做了详细的讨论……”

4. 规范场理论统一了四种基本力中的三种

杨-米尔斯的非交换规范场理论刚推出时并没有被人们所接受，因为它一时无法解决规范量子如何获取质量并实现重正化的问题。但由于其深刻的思想和简洁优美的数学形式，逐渐受到越来越多的关注，并且一步步取得成功，最后竟成为统一宇宙基本作用力的主流理论。

1960年代，美国物理学家格拉肖(Sheldon Lee Glashow，1932—)、温伯格(Steven Weinberg，1933—)和巴基斯坦物理学家萨拉姆(Abdus Salam，1926—1996)先后独立提出了由$SU(2)\times U(1)$李群变换所决定的杨-米尔斯规范场理论，用以统一描述弱力和电磁力作用。1971年，荷兰人霍夫特(Gerardus’t Hooft，1946—)和维尔特曼(Martinus J. G. Veltman，1931—)成功地在格拉肖-萨拉姆-温伯格的弱-电规范场论(简称为CWS理论)中引入希格斯机制，使其中的规范量子获得质量并实现重正

① R·米尔斯. 规范场. 自然杂志，1987，10(8)：563-577.

化，为该理论扫除了一大障碍。1973年，CWS理论预言的中性流被证实。1983年，在欧洲粒子物理研究中心工作的意大利人鲁比亚（Carlo Rubbia，1934—）与荷兰人范德米尔（Simon van der Meer，1934—）在质子-反质子对撞机上发现了CWS理论所预言的传递弱力作用的W粒子和Z粒子。至此，CWS理论已得到了完全确认。

格拉肖、萨拉姆和温伯格因成功建立了统一描述弱力和电磁力作用的规范场理论而分享了1979年诺贝尔物理学奖。鲁比亚和范德米尔因发现了CWS理论所预言的W粒子和Z粒子而分享1984年的诺贝尔物理学奖。霍夫特与维尔特曼则因解决了CWS理论的重正化问题而分享1999年诺贝尔物理学奖。

在强力作用方面，迄今为止，物理学家已通过粒子加速器和宇宙射线发现了300多种亚原子粒子。其中参与强相互作用的有100余种，被称为“强子”；强子中又分“重子”和“介子”；质子和中子都属于重子。美国物理学家盖尔曼（Murray Gell-Mann，1929—）在1961年提出，所有的强子都由一类更基本的粒子，叫做“夸克”，按“八重法”组成。他还于1964年发现，“八重法”的夸克模型遵循$SU(3)$李群变换的对称性。盖尔曼的理论被一系列实验结果证实。他因此获得了1969年诺贝尔物理学奖。

实验发现“夸克”具有一些奇怪的性质，那就是它们被永远禁闭在强子之中，不会单独出现；而且当夸克之间的距离很小时，它们相互的作用力反而会减小，被称为“渐近自由”。1973年，美国物理学家格罗斯（David J. Gross，1941—）、玻利泽（H. David Politzer，1949—）和维里茨克（Frank Wilczek，1951—）合

作,用数学方法建立了强作用力的 $SU(3)$ 杨-米尔斯规范场理论。根据该理论,每种夸克都带有“红”、“绿”、“黄”三种“颜色”之一;三个不同颜色的夸克合在一起形成“无色”的重子;带有互补颜色的一个正夸克和一个反夸克则形成“无色”的介子;并且夸克此时确实具有“渐近自由”的性质!他们于是创立了强作用力的规范场理论,被称作“量子色动力学”。由于他们的杰出贡献,格罗斯、玻利泽和维里茨克分享了 2004 年的诺贝尔物理学奖。

这样,杨-米尔斯规范场理论在创立了 50 年之后,已成为三种基本作用力的标准模型。

未来之舟

物理学家已相信,我们的世界确实是受非交换的规范场支配的。迄今为止,四大基本作用力中,只有引力尚未被纳入规范场理论。物理学家一直在探索能够包含引力的大统一的规范场理论。目前,最有希望获得成功的是“超弦”理论,这其实是十维空间上的规范场。

人们后来发现,规范场竟然与数学中的微分流形有紧密联系;而杨-米尔斯方程则已成为现代微分几何学强有力的研究工具(详见本书 2.3 节)。

1.5 发现那只“看不见的手”

——市场竞争平衡的数学理论

1969 年,诺贝尔经济学奖开始颁发。首届获奖者是挪威人拉格纳·弗里希(Ragnar Frisch,1895—1973)和荷兰人简·丁伯根(Jan Tinbergen,1903—1994)。他们发展了用动态模型来分析经济进程。前者是经济计量学的奠基人,后者是经济计量

学模式建造之父。如果说，这是数学和经济学紧密联系的开始，那么，为发现“看不见的手”作出努力的数学工作，更显示数学在经济学中的巨大作用。

1. 亚当·斯密提出“看不见的手”

18 世纪的苏格兰人亚当·斯密(Adam Smith,1723—1790)是西方经济学之父，他首创的市场经济的理论主导了西方社会 200 多年来的经济发展。在中国，虽然曾经拒绝过市场经济而坚持计划经济，现在也已实事求是地承认市场经济具有相当的活力，而给予其合法的地位。

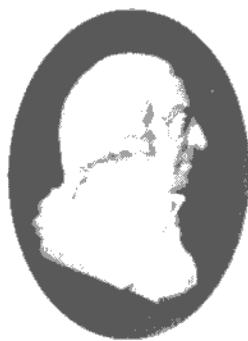


图 1-20　亚当·斯密

亚当·斯密在其 1776 年出版的名著《国富论》中断言：

> 在自由竞争的市场经济中，每个人(生产者和消费者)都只顾追求自己的最大利益；他们这样做时，却好像受到一只“看不见的手”支配，为增进社会的财富作出自己最大的贡献。

在亚当·斯密看来，自由竞争的市场机制表面上不受任何干预，其实受到了“看不见的手”强力控制，从而能够以最佳的方式为社会创造财富。

这只“看不见的手”其实就是调节供需平衡的价格杠杆：当某个商品供不应求时，其价格就上升，导致供应方为追逐利润而扩大生产，需求方则为了节省开支而减少购买，结果供应增加、

需求减少；当商品供大于求时，其价格就会下降，导致供应方转向生产其他更有利可图的商品，需求方则因价格便宜而增加购买，结果供应减少、需求增加。

曾在瑞士洛桑大学执教的法国经济学家瓦尔拉（Léon Walras，1834—1910）首先试图用数学的方式来表达亚当·斯密的思想。在其1874年出版的著作《纯粹经济学原理》中，瓦尔拉对每个商品定义了一个“需求函数”，以表示商品的需求量对于商品的价格、其他可替代商品的价格、消费者的收入与口味的依赖关系；还定义了一个“供应函数”，以表示商品的供应量对于商品的价格、生产成本以及生产技能的依赖关系。瓦尔拉利用这两种函数，建立起了表示市场供求关系的一组数学方程。于是，亚当·斯密的“看不见的手”论断，在此可以重新表达为：

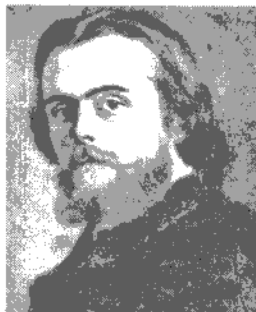


图1-21　瓦尔拉

> 每个人（消费者或生产者）都在可选择的范围内作出使自己获得最大经济效益的选择，结果将导致瓦尔拉市场的供需正好平衡。即存在这样的一组商品价格，它使得所有商品的需求函数和供应函数正好相等。

这样，瓦尔拉创立了一种重要的经济理论，叫做“一般均衡理论”。他也因此开创了西方经济学的一个重要学派——洛桑学派，也称为“数理学派”，该学派致力于用数学方法研究经济问题，特别关注一般均衡理论的研究。

2. 市场经济理论的数学化

在“一般均衡理论”这一名称中，“一般”意指市场中的所有的（而非个别的）商品；“均衡”即指商品的供需平衡。因此，该理论的研究重点，就是要找出正好使市场的供需保持平衡的所有商品的价格。但由于市场的情况极为复杂，在很多时候，瓦尔拉给出的那组数学方程无法求解；甚至有时求得负值的均衡价格，这显然没有实际意义。另一方面，瓦尔拉给出的数学模型也较粗糙，与实际情况相去甚远，因而受到质疑。在相当长的时期内，一般均衡理论的研究没有很大的进展。

直到 1939 年，英国牛津大学的经济学家希克斯（John Richard Hicks，1904—1989）在其著作《价值与资本》中，对一般均衡理论作出了重要的改进。他打破了原先单个市场的局限，提出多市场竞争平衡的数学模型，其中补充了信贷和现金等因素；并充分考虑了消费者和生产者的行为，使得模型与实际情况大为接近；特别是引入了资本理论，从而可以运用利润最大化方法，来研究消费和生产的变化规律。利用希克斯的模型，还可以探究当一些外界因素发生变化时——如消费者口味改变、农业收成起伏以及企业预期价格波动等——将会导致市场产生怎样的后果。



图 1-22　希克斯

希克斯由于对一般均衡经济理论的开拓性贡献，而荣获（与阿罗分享）1972 年的诺贝尔经济学奖。

然而，由于希克斯使用的是传统数学工具——微积分，所以，他仍然不能彻底解决市场的均衡价格是否存在的问题，也不能避免出现负值均衡价格的情况。

数学小知识 微积分是由17世纪的英国人牛顿(Isaac Newton，1642—1727)和德国人莱布尼茨(Gottfried Wilhelm Leibniz，1646—1716)发明的一种无穷小变量分析方法；它是解决自然界和工程技术问题的最强有力的工具；但它并不适用于经济领域，因为经济领域中的许多变量都具有非负性，这是微积分方法所难以控制的。

3. 艰深的数学进入经济学领域

1954年，困扰了西方经济学家近百年的一般经济均衡问题终于被彻底解决。作出这一重要贡献的是两位具有较深数学造诣的著名学者——阿罗(Kenneth J. Arrow，1921—)与德布鲁(Gerard Debreu，1921—)。

阿罗和德布鲁在他俩合作发表的论文“竞争经济均衡的存在性”中，使用了不同于以往的新数学工具。他们建立了一个抽象经济的模型：l 种商品构成了一个 l 维的向量空间。与之相对应的价格向量则形成了一个对偶空间；商品空间以及与之对偶的价格空间都是“拓扑”意义下的“凸集”。然后运用匈牙利数学家冯·诺依曼(John von Neumann，1903—1957)所创立的博弈论方法，并根据日本数学家角谷静夫(Kakutani Shizuo，1911—2004)所证明的凸空间上集值映射的不动点定理，在很一般的条件下，证明了均衡价格的存在性。



图 1-23　阿罗



图 1-24　德布鲁

200 多年前亚当·斯密所断言的那只“看不见的手”，现在终于显露了庐山真面目。

1972 年，阿罗由于“对一般经济平衡理论和福利理论的开拓性贡献”而与希克斯分享了该年的诺贝尔经济学奖。

德布鲁对于一般均衡的研究继续作出了一系列重要贡献。特别是，他在 1970 年，用微分拓扑的方法证明了：在所有的抽象经济的集合中，不满足均衡唯一性（即存在多个均衡价格）的点可以忽略不计，因而解决了又一个令人困扰的经济理论问题。他在 1959 年出版的著作《价值理论：对经济均衡的公理化分析》，把一般均衡的经济理论彻底纳入数学公理化的框架中。该书已成为数理经济学中的一部经典名著。

1983 年，德布鲁由于“在经济理论中引入新的（数学）分析方法，并对一般均衡理论进行了严格的重构”的成就，而独享了该年的诺贝尔经济学奖。

数学小知识　“凸集”或“凸空间”是指几何空间中的一类点集，其特征是每个“凸集”都包含了以该集中任意两点为端点的线段；“拓扑学”是研究几何结构连通性质的数学分支；“微分拓

扑”用微积分方法研究几何对象的拓扑性质，是拓扑学的分支；“不动点定理”揭示，定义在几何空间上的映射如何将空间中的某一点(集)仍然映成该点(集)。

4. 数学科班出身

阿罗出生于美国纽约市，1940 年获纽约市立学院数学学士学位；1941 年获哥伦比亚大学数学专业的硕士学位。1942—1946 年，因第二次世界大战爆发而中断学业去参军，担任气象预报军官。战后加入芝加哥大学的考尔斯经济研究委员会，任助理研究员；同时在哥伦比亚大学攻读博士学位，其博士论文就是那篇用数学公理化方法研究福利经济学问题的文章(参见本书 1.6 节)。后到哈佛大学任经济学教授。

德布鲁出生于法国加莱市，曾在加莱市学院读书。1939 年，法国因卷入第二次世界大战而局势动荡。德布鲁只能进入一个临时数学学校求学。1941—1944 年进入著名的法国巴黎高师，在那里学到了丰富的数学知识，并对当时名震一时的布尔巴基学派以及他们所倡导的数学公理化思想留下了深刻印象。在被短暂征入军队又退役之后，于 1945 年通过了法国数学教师的资格考试，并开始对经济学研究发生兴趣。1948 年赴美国访问。1949 年受芝加哥大学考尔斯经济研究委员会的聘请任助理研究员，从此在美国定居。后曾在多个美国和欧洲的大学或研究所任职。

未来之舟

由德布鲁所创立的公理化一般均衡理论已成为微观经济学的基础，被

广泛应用于生产理论、金融理论和国际贸易理论等研究。而由阿罗和德布鲁所开创的公理化方法，已经成为经济分析的标准形式：其他一些经济学分支，如宏观经济学、工业组织和公共财政理论等，也已被公理化。

1.6　公理化的个人利益与社会选择

古希腊的奴隶主民主政治催生了公理化的几何证明，民主投票中又出现了一连串的数学问题。数学与民主有着天生的密切联系。这里叙述的是一个出人意料的数学故事。

1.“投票悖论”

一个社会经常要做出各种选择，如控制物价，调节税收，分配财富，选举总统，签订条约，甚至宣布战争，等等。对于生活在社会中的个人来说，社会所做的选择与他/她个人的利益可能一致也可能冲突。

那么，社会选择是如何做出的？根据不同的社会制度和不同性质的问题，选择的方式也不同：有的场合按照大多数人的利益和意志做出社会选择，如通过投票做政治决定，通过市场机制作经济决定；有的场合则由少数人意志甚至个人独裁做出社会选择；还有的场合则根据传统或宗教法典，按照“神”的意志做出决定。

考察社会选择与个人利益之间的关系，这属于福利经济学的研究领域。福利经济学创建于20世纪初的英国，其目的是从福利效用最大化的原则出发，对各种经济政策进行评价。对于福利经济学家来说，福利就是个人对于自己社会和经济地位的

满足感。福利效用最大化,就是让最多的人得到最大的满足。

因此,使社会选择与个人利益尽可能一致,显然有助于提高社会福利的效用。

所以,根据大多数人的意志,即民主方式,来决定社会选择,应该是增进社会福利的最佳方法。但人们发现,这种方法有时会产生不合理的结果。18 世纪法国思想家孔多塞(Marquis de Condorcet,1743—1794)就曾提出如下著名的“投票悖论”。

假设有甲、乙、丙三人组成的社会,面对 A、B、C 三个选择方案,他们的偏好顺序分别如下。

甲:A 好于 B,B 好于 C(从而 A 好于 C);

乙:B 好于 C,C 好于 A(从而 B 好于 A);

丙:C 好于 A,A 好于 B(从而 C 好于 B)。

则根据少数服从多数的投票原则,社会的选择将是 A 好于 B,B 好于 C。这样,如果社会的选择是合理的,那么应该认为 A 好于 C。但投票结果却是 C 好于 A。也就是说,合理的个人选择,通过投票选举得到了不合理的社会选择。

“投票悖论”看来与人们的直觉矛盾。为什么会出现这种情况?有没有办法,比如说,采用一种更复杂的投票程序,来避免这种情况?经济学家和社会学家长期困惑于这一问题。直到 1950 年,美国数学家和经济学家阿罗运用数学公理化方法,对一些概念作了明确的定义,并进行严密的论证,终于澄清了整个问题。

2. 阿罗的“社会福利”公理

公理化方法始于 2 300 多年前希腊数学家欧几里得(Euclid,活动于公元前 300 年)的著作《几何原本》。该书在开头给出 23 个定义、5 条公设和 5 条公理,然后通过逻辑推理证明了 465 个命题,演绎出整个几何学体系。


图 1-25 欧几里得

欧几里得几何的影响深远,直到今天,全世界的中学生仍然在课堂上学习这种几何。欧几里得的公理化思想更被发扬光大,特别是在 20 世纪初,由于德国数学家希尔伯特(David Hilbert,1862—1943)和英国数学家罗素(Bertrand Arthur William Russell,1872—1970)对于数学基础研究的卓越贡献,使得公理化方法成为现代数学研究的基本方法。

数学小知识 通俗地讲,所谓公理就是那些被人们普遍接受、公认是正确的判断和条件;定理则是以公理为前提通过逻辑推理得到的结论;推论又是从定理推理而得。显然,只要前提正确、推理无误,那么所得的结论必然正确。所以公理的正确性保证了定理和推论的正确性。数学和几何所以被认为是严密的可靠的科学,公理化方法在其中起着关键的作用。

阿罗从高中时代就通过罗素的数理逻辑名著,对公理化思想有了深入了解,并对它着了迷。他于是在 1950 年的博士论文


图 1-26　阿罗

“社会福利概念的难题”①中，尝试用公理化方法来研究个人利益与社会选择的问题。

阿罗首先定义了一个供个人和社会作选择的备选对象的集合 S，然后定义在 S 上的一种序关系 R，这相当于个人或社会对 S 中所有的元素作了一个孰优孰劣的选择。序关系 R 必须满足两个公理。

公理 1(完全性)　对于 S 中任意的两个备选对象 x,y，必然有 xRy 或 yRx。

其中 xRy 可理解为“根据 R 的选择，x 不劣于 y”(相当于“x 好于 y”或“x 和 y 一样好”)。公理 1 是说对于任意两个备选对象，总可以比较其优劣。

公理 2(传递性)　对于 S 中任意的三个备选对象 x,y,z，由 xRy 和 yRz，可以推出 xRz。

此公理的含义为：对于 S 上的选择 R 来说，如果认为 x 不劣于 y，y 不劣于 z，那么必然认为 x 不劣于 z。这种传递性质显然是每一个合理选择都应该具备的。

阿罗接着定义了社会福利函数的概念。

定义　一个“社会福利函数”是指一个过程或规则，它对于备选对象集 S 上的个人序集合 $\{R_1,R_2,\cdots,R_n\}$，给出对应的一个

---

① 该论文在第二年以《个人价值与社会选择》为书名出版。

社会序 R。

即社会福利函数就是给出一个如何汇集所有的个人选择以得到社会选择的过程或规则。社会中每个人的利益和意志显然可以从其个人选择中得到体现。因此，此处定义的社会福利函数反映了前述的社会福利效用。

我们当然希望这个福利函数具有“公平”、“合理”和“民主”等性质。阿罗于是给出了能够刻画此类福利函数的4个条件。

条件1 社会福利函数定义在所有的可容许的个人序关系之上。

即社会福利函数本身不能对个人选择的范围进行限制：个人的任何选择都是可容许的，只要该选择的序关系满足前述的公理1和2，并且符合与人类本性和经验有关的一些先验条件。这相当于在民主社会中，不能限制个人的选择自由。

条件2 社会福利函数遵守“帕莱托原则”。

即对于任意两个备选对象 x,y，如果社会中每一个人都认为 x 好于 y，那么由社会福利函数规定的社会选择也必须认为 x 好于 y。既然我们定义的是社会“福利”函数，而不是“祸害”函数，所以这一条件理所当然要满足。该条件由意大利经济学家帕莱托(Vilfredo Pareto,1848—1923)首先提出。

条件3 社会福利函数独立于无关的备选对象。

比如说，如果社会福利函数给出的社会选择认为在“控制房价，增加工资”这两个备选对象中，“控制房价”好于“增加工资”，

那么它在“控制房价，增加工资，银行加息”这三个备选对象中，将仍然认为“控制房价”好于“增加工资”。这里，“银行加息”就是无关的备选对象。

条件 4 社会福利函数不是独裁的。

即在社会中不存在个人 i，使得福利函数给出的社会选择 R 总与这个人的选择 R_i 一致。

这 4 个条件显然是一个“合理、公平和民主”的社会福利函数所必须具备的基本条件。但阿罗运用逻辑推理的方法证明：同时满足这 4 个条件的社会福利函数是**不存在**的。这就是著名的“阿罗不可能定理”。

根据这一定理立即得到这样的推论：以民主程序产生的社会选择必然不具有合理性。或者等价地，一个能产生合理社会选择的程序或规则必然是“独裁的”。这也表明，“投票悖论”不可能避免。

阿罗的结果出人意料，但由于用公理化的严格推理方式得来，所以不能不承认它的正确性。这在当时的西方学术界引起强烈反响。一些学者感叹道，阿罗定理又一次显示了常识多么容易出错。

阿罗的工作为福利经济学开辟了新的研究方向，提供了新的研究方法。1972 年，阿罗由于“对一般经济平衡理论和福利理论的开拓性贡献”，而与别人分享了该年的诺贝尔经济学奖。

3. 进一步的发展

为了破解“阿罗不可能定理”所造成的“民主”与“理性”不能

共存的两难局面，福利经济学家们开始对社会选择问题进行更深入的探讨，他们仍然使用由阿罗提供的公理化方法。其中，在英国剑桥大学三一学院任教的印度经济学家阿马蒂亚·森(Amartya Sen，1933—)获得的研究结果最引人注目。

由于公理化方法的严密性，所以要想改变“阿罗不可能定理”的结果，只有适当放宽作为该定理逻辑前提的一些公理和条件。其中关于福利函数的 4 个基本条件显然不能再放宽。阿马蒂亚·森于是想到对公理 2 作修改。他提出用“社会决定函数”来代替阿罗的“社会福利函数”。



图 1-27　阿马蒂亚·森

定义　一个“社会决定函数”是指一个过程或规则，它对于备选对象集 S 上的个人序集合 $\{R_1, R_2, \cdots, R_n\}$，给出对应的一个 S 上的社会选择 R，使得 R 在 S 的每一个非空子集中总能找到“最好的”备选对象。

即对于“社会决定函数”所给出的社会选择 R 来说，它总能在任意一组备选对象中找到“最好的”那一个。阿马蒂亚·森证明了，当被选对象集 S 是有限集时，“社会福利函数”就是“社会决定函数”；但反之不然，因为“社会决定函数”所给出的社会选择 R 不一定满足上述的公理 2，即不一定具有传递性。

所以，“社会决定函数”的合理性稍差。但它使得我们的社会在任何情况下总能够选择“最好的”备选对象，这在绝大部分场合已经足够了。最重要的是，阿马蒂亚·森证明了，“社会决定函数”能够完全满足阿罗的 4 个条件，而且这些条件甚至可以

进一步加强，从而使社会选择的民主性得到更充分的保证。以上这些结果被称为“阿马蒂亚·森可能性定理”。

阿马蒂亚·森由于“对福利经济学的贡献”而独享了1998年的诺贝尔经济学奖。

未来之舟

由于阿罗和阿马蒂亚·森的卓越工作，社会选择理论的应用范围已不仅限于福利经济学，而是正在向人类各个社会活动领域扩展。在现代社会中，经常采用不同的方法来汇集个体选择以得到社会/群体选择。比如说，体育比赛中，汇集裁判打分以决定选手名次；电视台的群众娱乐节目中，综合评委的打分和观众的选票来取舍参赛者；企业公司里，代表股东利益的董事会要进行市场决策；在各级人大会议上，规定重要决议须有2/3多数同意才可通过；在联合国安理会上，5个常任理事国拥有“一票否决”权，等等。运用公理化的社会选择理论，可以对这些决策方式的“客观性”和“公正性”等作出严格准确的分析和评价，并且能够设计出最佳的社会/集体选择的方案。

1.7 “华尔街革命”[①]

狭义的金融学是指金融市场的经济学。现代意义下的金融市场至少已有300年的历史，它从一开始就是经济学的研究对象。但人们通常认为现代金融学只有不到50年的历史。这50

---

① 本节文字为著名数学家、金融数学家史树中教授所作。史教授1961年在华东师范大学数学系毕业后留校工作，和本书编者共事十余年。后来先后在南开大学、北京大学光华管理学院任教，是我国数理经济学的一位开拓者。2008年不幸病逝。为了纪念他的贡献，也为了使本书增色，特选刊他在2000年上海《科学》杂志第六期上的一篇文章。原题是“从数理经济学道数理金融学的百年回顾”。这里刊载的是文章的第二部分。

年也就是使金融学成为可用数学公理化方法架构的历史。

从瓦尔拉-阿罗-德布鲁一般经济均衡体系的观点来看,现代金融学的第一篇文献是阿罗于 1953 年发表的论文“证券在风险承担的最优配置中的作用”。在这篇论文中,阿罗把证券理解为在不确定的不同状态下有不同价值的商品。这一思想后来又被德布鲁所发展,他把原来的一般经济均衡模型通过拓展商品空间的维数来处理金融市场,其中证券无非是不同时间、不同情况下有不同价值的商品。但是后来大家发现,把金融市场用这种方式混同于普通商品市场是不合适的。原因在于它掩盖了金融市场的不确定性本质。尤其是其中隐含着对每一种可能发生的状态都有相应的证券相对应,如同每一种可能有的金融风险都有保险那样,与现实相差太远。

这样,经济学家又为金融学寻求其他的数学架构。用新的数学来架构的现代金融学被认为是两次“华尔街革命”的产物。第一次“华尔街革命”是指 1952 年马科维茨的证券组合选择理论的问世。第二次“华尔街革命”是指 1973 年布莱克-肖尔斯期权定价公式的问世。这两次“革命”的特点之一都是避开了一般经济均衡的理论框架,以至在很长时期内都被传统的经济学家认为是“异端邪说”。但是它们又确实使以华尔街为代表的金融市场引起了“革命”,从而最终也使金融学发生根本改观。马科维茨因此荣获 1990 年诺贝尔经济学奖,肖尔斯(M. Scholes,1941—)则和对期权定价理论作出系统研究的默顿一起荣获 1997 年的诺贝尔经济学奖。布莱克(F. Black,1938—1995)不幸早逝,没有与他们一起领奖。

马科维茨研究的是这样一个问题:一个投资者同时在许多种证券上投资,那么应该如何选择各种证券的投资比例,使得投资收益最大,风险最小。马科维茨在观念上的最大贡献,在于他把收益与风险这两个原本有点模糊的概念明确为具体的数学概念。由于证券投资上的收益是不确定的,马科维茨首先把证券的收益率看做一个随机变量,而收益定义为这个随机变量的均值(数学期望),风险则定义为这个随机变量的标准差(这与人们通常把风险看做可能有的损失的思想相差甚远)。于是,如果把各证券的投资比例看做变量,问题就可归结为怎样使证券组合的收益最大、风险最小的数学规划。对每一固定收益都求出其最小风险,那么在风险-收益平面上,就可画出一条曲线,它称为组合前沿。

马科维茨理论的基本结论是:在证券允许卖空的条件下,组合前沿是双曲线的一支;在证券不允许卖空的条件下,组合前沿是若干段双曲线段的拼接。组合前沿的上半部称为有效前沿。对于有效前沿上的证券组合来说,不存在收益和风险两方面都优于它的证券组合。这对于投资者的决策来说自然有很重要的参考价值。

马科维茨理论是一种纯技术性的证券组合选择理论。这一理论是他在芝加哥大学的博士论文中提出的。但在论文答辩时,它被一位当时已享有盛名、后以货币主义而获 1976 年诺贝尔经济学奖的弗里德曼(M. Friedman,1912—2006)斥之为“这不是经济学”! 为此,马科维茨不得不引入以收益和风险为自变量的效用函数,来使他的理论纳入通常的一般经济均衡框架。

马科维茨的学生夏普(W. Sharpe,1934—)和另一些经济学家,则进一步在一般经济均衡的框架下,假定所有投资者都以这种效用函数来决策,从而导出全市场的证券组合收益率是有效的以及所谓资本资产定价模型。夏普因此与马科维茨一起荣获 1990 年诺贝尔经济学奖。另一位 1981 年诺贝尔经济学奖获得者托宾(L. Tobin,1918—2002)在对于允许卖空的证券组合选择问题的研究中,导出每一种有效证券组合都是一种无风险资产与一种特殊的风险资产的组合(它称为二基金分离定理),从而得出一些宏观经济方面的结论。

在 1990 年与马科维茨、夏普一起分享诺贝尔经济学奖的另一位经济学家是新近刚去世的米勒。他与另一位在 1985 年获得诺贝尔经济学奖的莫迪利阿尼(F. Modigliani,1918—2003)一起在 1958 年以后发表了一系列论文,探讨“公司的财务政策(分红、债权/股权比等)是否会影响公司的价值”这一主题。他们的结论是:在理想的市场条件下,公司的价值与财务政策无关。这些结论后来就被称为莫迪利阿尼-米勒定理。他们的研究不但为公司理财这门新学科奠定了基础,并且首次在文献中明确提出无套利假设。

所谓无套利假设,是指在一个完善的金融市场中,不存在套利机会(即确定的低买高卖之类的机会)。因此,如果两个公司将来的(不确定的)价值是一样的,那么它们今天的价值也应该一样,而与它们的财务政策无关;否则人们就可通过买卖两个公司的股票来获得套利。达到一般经济均衡的金融市场显然一定满足无套利假设。这样,莫迪利阿尼-米勒定理与一般经济均衡

框架是相容的。

但是，直接从无套利假设出发对金融产品定价，则使论证大大简化。这就给人以启发，不必非要背上沉重的一般经济均衡的十字架不可，从无套利假设出发就可为金融产品的定价得到许多结果。从此，金融经济学就开始以无套利假设作为出发点。

以无套利假设作为出发点的一大成就也就是布莱克-肖尔斯期权定价理论。所谓(股票买入)期权是指以某个固定的执行价格在一定的期限内买入某种股票的权利。期权在它被执行时的价格很清楚，即：如果股票的市价高于期权规定的执行价格，那么期权的价格就是市价与执行价格之差；如果股票的市价低于期权规定的执行价格，那么期权是无用的，其价格为零。现在要问：期权在其被执行前应该怎样用股票价格来定价？

为解决这一问题，布莱克和肖尔斯先把模型连续动态化。他们假定模型中有两种证券，一种是债券，它是无风险证券，也是证券价值的计量基准，其收益率是常数；另一种是股票，它是风险证券，沿用马科维茨的传统，它也可用证券收益率的期望和方差来刻画，但是动态化以后，其价格的变化满足一个随机微分方程，其含义是随时间变化的随机收益率，其期望值和方差都与时间间隔成正比。这种随机微分方程称为几何布朗运动。然后，利用每一时刻都可通过股票和期权的适当组合对冲风险，使得该组合变成无风险证券，从而就可得到期权价格与股票价格之间的一个偏微分方程，其中的参数是时间、期权的执行价格、债券的利率和股票价格的“波动率”。出人意料的是，这一方程居然还有显式解。于是布莱克-肖尔斯期权定价公式就这样问

世了。

与马科维茨的遭遇类似，布莱克-肖尔斯公式的发表也困难重重地经过好几年。与市场中投资人行为无关的金融资产的定价公式，对于习惯于用一般经济均衡框架对商品定价的经济学家来说很难接受。这样，布莱克和肖尔斯不得不直接到市场中去验证他们的公式。结果令人非常满意。有关期权定价实证研究结果先在 1972 年发表，然后理论分析于 1973 年正式发表。与此几乎同时的是芝加哥期权交易所也在 1973 年正式推出 16 种股票期权的挂牌交易（在此之前期权只有场外交易），使得衍生证券市场从此蓬蓬勃勃地发展起来。布莱克-肖尔斯公式也因此有数不清的机会得到充分验证，而使它成为人类有史以来应用最频繁的一个数学公式。

布莱克-肖尔斯公式的成功与默顿的研究是分不开的，后者甚至在把他们的理论深化和系统化上作出更大的贡献；默顿的研究后来被总结在 1990 年出版的《连续时间金融学》一书中。对金融问题建立连续时间模型也在近 30 年中成为金融学的核心。这如同连续变量的微分学在瓦尔拉斯时代进入经济学那样，尽管现实的经济变量极少是连续的，微分学能强有力地处理经济学中的最大效用问题；而连续变量的金融模型，同样使强有力的随机分析更深刻地揭示金融问题的随机性。

不过，用连续时间模型来处理金融问题并非从布莱克-肖尔斯-默顿理论开始。1950 年代，萨缪尔森就已发现，一位几乎被人遗忘的法国数学家巴施里叶（Bachelier，1870—1946）早在 1900 年已在其博士论文《投机理论》中用布朗运动来刻画股票的

价格变化,并且这是历史上第一次给出的布朗运动的数学定义,比人们熟知的爱因斯坦(A. Einstein,1879—1955)1905 年的有关布朗运动的研究还要早。尤其是,巴施里叶实质上已开始研究期权定价理论,而布莱克-肖尔斯-默顿的工作其实都是在萨缪尔森的影响下,延续了巴施里叶的工作。这样一来,数理金融学的"祖师爷"就成了巴施里叶。对此,法国人感到很自豪,最近他们专门成立了国际性的"巴施里叶协会"。2000 年 6 月,协会在巴黎召开第一届盛大的"国际巴施里叶会议",以纪念巴施里叶的论文问世 100 周年。

1.8 线性规划的传奇故事

线性规划诞生于 1938 年苏联的列宁格勒(圣彼得堡),但是真正开花结果却在第二次世界大战之后的美国。现在线性规划已经进入数学教材。它的传奇经历发人深思。

1. 线性规划的计算机求解成为世界头版新闻

1979 年 11 月 7 日,美国《纽约时报》头版报道,俄罗斯青年数学家哈奇扬(Leonid Khachiyan,1952—2005)的一项发现"震动了数学和计算机科学界":他找到了线性规划的一个有效算法——"椭圆算法",能够大幅度地减少复杂问题的计算量。

1984 年 11 月 19 日,《纽约时报》又在头版报道,美国电话电报公司贝尔实验室的印度青年数学家卡马卡(Narendra Karmarkar,1957—)取得"惊人的理论突破":他所发现的线性规划

算法——“内点法”，无论是在简单情况还是在复杂情况下都比通常算法快得多。

报纸媒体通常很少报道数学新闻，因为数学太抽象且远离现实，很难会引起普通读者的兴趣。那么，《纽约时报》为何如此关注数学家对于线性规划的研究进展？

线性规划就是在线性约束条件下求线性目标最优解的理论和算法。它隶属于应用数学领域运筹学分支，在生产、运输、资源分配等经济领域中有着广泛的应用。线性规划看起来十分简单，但效益惊人。在实际应用中，一般可在不增加任何成本的情况下，使产品产量或工作效率提高 10%以上。美国的一些银行和石油公司都曾经因搞线性规划而发了财。

线性规划最常用的解题算法是“单纯形法”，该算法通常很有效。但遗憾的是，它后来被发现是一个“坏”算法。这就是说，随着待解问题的变量个数增加，“单纯形法”的计算时间可能会以指数级倍数增长，将很快超出最强大计算机的能力。

数学家多年来一直在研究线性规划是否存在“好”算法，即计算时间按变量个数的多项式倍数增加的算法。无论从理论还是从实践角度来看，这一研究都具有非常重要的意义。

哈奇扬终于找到被证明是“好”算法的线性规划“椭圆算法”，解决了一个长期悬而未决的数学难题，因而引起了数学界和计算机科学界的震动。不过，实际检验表明，当变量个数少于 5 000时，单纯形法还是比椭圆算法快。

而卡马卡发现的内点算法则不仅在理论上被证明是一个“好”算法，而且实验证明要比单纯形法快 50 倍左右。美国电话

电报公司要改造州际电话网，其中涉及计算一个具有80万个以上变量的线性规划，如使用其他算法则需要数周时间，使用卡马卡算法不到10小时就可以完成。

鉴于线性规划具有如此重要的经济意义，引起《纽约时报》的关注也不足为奇了。

其实，线性规划开始时远没有如此风光。它曾经备受轻视和冷落。由于一些杰出数学家和经济学家的努力和坚持，终于使它发展为一门举足轻重的经济学与数学交叉的学科。

2. 线性规划在苏联的遭遇

苏联人坎托罗维奇（Леонид Витальевич Канторович，1912—1987）是一位极有天赋的纯粹数学家①。他14岁就考入列宁格勒大学数学系，18岁毕业，22岁已升任列宁格勒大学教授；在数学的一个重要分支领域——泛函分析——中获得多项优秀研究成果。



图 1-28　坎托罗维奇

不同于其他纯粹数学家的是，坎托罗维奇不仅专注于研究数学本身，而且非常关心数学在其他领域的应用。1938年，26岁的他接手了当地一家木材加工联合企业向列宁格勒大学数学系的求助：要求为8台具有不同生产能力的机床制订工作程序表，以使其按一定比例配套生产的5种胶合板的总产量达到最

① 一般把数学分为纯粹数学和应用数学，详见本书第2章的介绍。

大。用数学解题的语言来说：

有 8 台机床和 5 种胶合板，已知第 $i(1\leqslant i\leqslant 8)$ 台机床对第 j $(1\leqslant j\leqslant 5)$ 种胶合板的生产率（数值表略），要求分配第 i 台机床对第 j 种胶合板的产量，使得胶合板的总产量达到最大，其中规定 5 种胶合板产量的比例分配为 10%，12%，28%，36%，14%。

坎托罗维奇仔细地分析了这一问题，发现它可以归结为在一组线性约束条件下求最优解的问题。这种问题与传统的数学问题有较大区别，当时并没有现成的解决方法。坎托罗维奇于是引入了“解乘数”的概念以求得问题的最优解。

坎托罗维奇进一步发现，一大类经济领域中的问题都可以用同样的方法解决。比如说，最充分地利用机器设备，最大限度地利用原料并减少残料，最合理地利用燃料，建筑材料的最优分配，农田播种面积的最优安排以及运输最优规划等等。

坎托罗维奇把他的研究结果写成一本小册子，题名为《生产组织和计划中的数学方法》，此书被公认是线性规划的诞生标志。

然而，坎托罗维奇的成果在当时几乎遭到了来自所有方面的反对：数学家反对，因为它看上去太简单，没有什么学术价值；企业管理人员反对，因为它限制了他们制订生产计划的自由，威胁到他们的管理权威；甚至企业工人也反对，因为它将减少边角料的回收，因而影响他们的奖金收入。

经济学界认为，线性规划“需要大量数据，实际中可没有”；“原始数据在许多场合下都值得怀疑，据此选择的计划不一定是最优的”，有的甚至说，坎托罗维奇建议在经济计划中使用数学

规划是“侵犯了计划工作员的选择自由，同时使苏联的计划经济中依靠传统的算术方法进行实物形态的资源分配而达到的高速度经济增长受到威胁”，由于苏联计划经济工作者和经济学家的“恐数学症”，线性规划在苏联的广泛应用至少推迟了20年。

随着线性规划在西方社会的兴起，终于使苏联当局认识到坎托罗维奇工作的价值，从而开始支持他全面推动数学在经济领域中的应用。坎托罗维奇后来当选为苏联科学院院士，并获得列宁勋章。

3. 线性规划在美国

库普曼(Tjalling Charles Koopmans，1910—1985)出生于荷兰的斯格莱夫兰；其父母均为教师，非常重视对子女的教育；17岁考入乌德勒支大学，学习数学和物理学；1933年获硕士学位后，因“希望研究更接近生活的事物”而改学数理经济学，1936年在列登大学获博士学位；1940年为避纳粹德国的战祸而移居美国。



图1-29　库普曼

1942年，库普曼任华盛顿特区英国商船使团的统计员，其任务是为船队制订运输方案。具体地说：

> 有数千条商船，要在数百个世界各地港口之间航行，运载数百万吨货物。要求制订的运输方案能保证空船行驶的航程最少，并使运输成本最低。

为了完成这一复杂的任务，库普曼发展了一套叫做“活动分

析”的方法，这其实也是线性规划。为了获得最优方案，库普曼还引入了“影子价格”的概念，它相当于坎托罗维奇的“解乘数”。

由于战争，库普曼的论文当时被保密，多年后才得以公开。

战后，库普曼对于推动线性规划在经济领域中的应用发挥了关键作用。他积极支持丹齐克发明的“单纯形法”，并与后者一起商定使用“线性规划”这一词；他数次发起召开线性规划研讨会，促进了这一新学科的传播；他还带头与苏联学者进行学术交流，使坎托罗维奇的开创性工作得以广为人知。

美国人丹齐克(George Bernard Dantzig，1914—2005)在数学家父亲的引导下从小就喜欢上数学。他 1936 年毕业于马里兰大学数学系，1938 年获该大学的数学专业硕士学位。1939 年入加利福尼亚大学贝克莱分校，师从著名的数理统计学家耐曼(Jerzy Neyman，1894—1981)攻读博士学位。

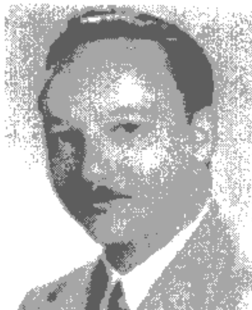


图 1-30　丹齐克

有一天，迟到的丹齐克走进教室，只看见黑板上有两道统计题目，以为是耐曼布置的作业，就抄下来带回家做。他发现这两道题特别难，但花了几天工夫之后，还是设法把它们做出来了。交给耐曼后他才知道，它们其实是当时尚未解决的统计学难题。这两道题后来成为丹齐克博士论文的主要内容，并且与他后来发明的线性规划模型有直接联系。

第二次世界大战中断了丹齐克的学业。1941 年，他加入美国空军，在统计控制室下的战斗分析小组负责数据收集和处理

工作。战争结束后，他回到大学，完成了博士论文答辩。不久，又重新被空军招募，担任计算控制室首席数学家。

丹齐克在空军主要负责优化军队的各方面工作程序，包括飞行员调配、飞机部署、训练安排、后勤供应等。有时候还要处理“士兵配餐”之类的问题。

为了保证士兵的营养，规定每餐食品必须定量含有各种营养成分，例如蛋白质、脂肪、碳水化合物、无机盐、维生素和纤维素等。这些营养成分可以由各种不同的食品来提供，例如牛奶和鸡蛋提供蛋白质和维生素，牛排和猪肉提供蛋白质和脂肪，胡萝卜和青菜提供维生素和纤维素等。约有数百种食品，其价格不一。要求决定一份套餐中的食品搭配，以较低的成本满足营养成分的需要。

1947年，丹齐克为他所要解决的所有这些问题建立起一个通用的数学模型，并找到了一个十分有效的算法——“单纯形法”。为了构建他的模型和算法，丹齐克曾经向好几位杰出的数学家和经济学家请教。特别是，他得到了著名数学家、计算机理论奠基者和博弈论创立人冯·诺依曼的很大帮助。同时，他还从库普曼那里得到支持和鼓励。“线性规划”这一词，就是丹齐克和库普曼一起商定使用的。

由于种种原因，坎托罗维奇和库普曼的工作在相当长的时间内不为人知。而丹齐克所创立的模型更具有一般性，算法更有效，所以很快流传，并最终成为线性规划的标准内容。丹齐克因此而被许多人称为“线性规划之父”。

4. 终于获得诺贝尔经济学奖

1975 年，坎托罗维奇和库普曼因“对资源最优分配理论的贡献”而分享了该年的诺贝尔经济学奖。

从瑞典皇家科学院的本策尔(Ragnar Bentzel)教授的授奖发言中可以看出，这次诺贝尔经济学奖是为了表彰线性规划在经济领域中的成就。许多人对同样为线性规划作出重要贡献的丹齐克未被列入获奖名单而感到不平。获奖人之一库普曼后来也在多种场合表示强烈不满，他甚至拿出了三分之一的获奖金额以丹齐克的名义捐给了位于奥地利拉克森堡的“应用系统分析国际研究所”(IIASA)。三位线性规划创始人经常在 IIASA 会面，进行学术交流(图 1-31)。在库普曼和坎托罗维奇的获奖演说中，都提到了丹齐克对线性规划的重要贡献。

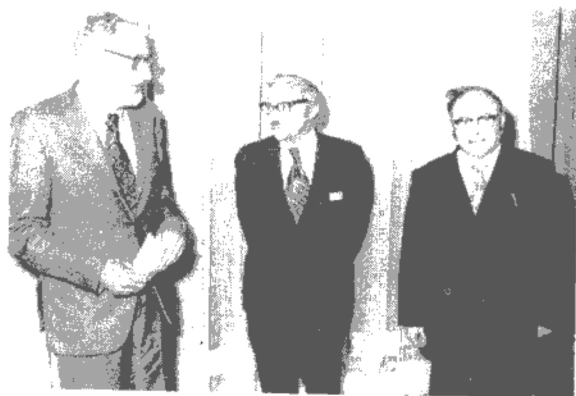


图 1-31　库普曼、丹齐克与坎托罗维奇在 IIASA

对于丹齐克本人来说，值得欣慰的是，就在同一年，他“因发明线性规划和发现单纯形法”而获得了由美国总统颁发的美国国家科学奖，并获得了由美国运筹学会颁发的首届冯·诺依

曼奖。

5. 线性规划在中国

1958年，在“大跃进”的情势下，数学界掀起“理论联系实际”，“数学直接为国民经济服务”之风。纯粹数学和应用数学很难直接进入经济部门和企业发展。这时，“线性规划”就像一道闪电，打开了中国数学家的眼界。数学居然能直接为国民经济服务。于是，在华罗庚的率领下，万哲先、越民义、王元、吴方、朱永津等一大批中国科学院数学所的数学家(不少人是华的学生)，以及山东师范学院、曲阜师范学院的一些教师也投入其中，并取得了应用和理论成就。如万哲先创立了“图上作业法”；越民义给出了“表上作业法”一个证明；管梅谷受“图上作业法”的启示，根据欧拉(L. Euler，1707—1783)关于奇偶点的理论，给出了最短路线的一个类似于“图上作业法”的判别法。与此相应，吴文俊则带领另一帮数学家另辟蹊径，开创了中国现代对策论(博弈论)研究。

1960年秋，在中共北京市委农村工作部的统一领导下，中科院数学所、力学所、中国科技大学、北京师范学院、北京农机学院、北京师范专科学校、北京工农师范学院等7个单位的部分师生，参加了北京市郊的麦收。华罗庚也下去了解了情况，取得了第一手资料，并用运筹学(主要是图上作业法)对打麦场问题进行了现场研究。1960年冬，当轰轰烈烈的“线性规划”研究活动逐渐冷却下来的时候，华罗庚又尝试了“矿体几何学”和蒙特卡罗(Monte-Carlo)方法的应用研究，并和王元一起出版了一本小

册子。这一时期，华罗庚一直考虑如何把数学方法应用到国民经济中，应用到管理上去的问题，目的是希望“从我国的实际出发搞出一套适合我国国情的、行之有效的管理科学！”为此，华罗庚 1959 年 5 月 28 日在《人民日报》上发表了《大哉数学之为用》的文章；1960 年在《光明日报》上发表《运筹学》一文；1960 年 2 月 26 日至 9 月 27 日，在《人民日报》上发表了《数学的用场》五则和 10 月 30 日发表《数学工作者要大力为农业服务》的文章，确立了“牢记把方法交给群众”这一思想，为日后推广“优选法和统筹法”的应用奠定了思想基础。

未来之舟

由于线性规划取得了惊人成功，吸引了众多数学家来关注经济领域中种种最优化规划的问题，从而形成了“数学规划”这门应用数学新学科。该学科除了包括线性规划之外，还包括非线性规划、整数规划、组合规划、动态规划和多目标规划等，其所研究问题的范围和难度已远远超出了线性规划。

1.9　博弈论在经济领域中的应用

“世事如棋”①，这句古语恰当地形容了人类在社会活动中彼此争斗的一面。这种争斗在军事、政治、外交、经济、体育竞技等领域尤为突出。争斗的参与者可以是个人、团体和国家，争斗对手可以是双方或者多方。虽然争斗的内容和形式千变万化，但都与赌博和下棋有相通之处，那就是要遵守一定的规则并讲

---

① 出自[宋]·僧志文的诗。

究策略制胜。故常以“博弈”来代指人类之间的各种争斗。

1. 策略制胜

所谓策略就是博弈者根据自己和对手的情况以及当前的局面,为获取自身利益而采取的行动步骤。以策略制胜的一个典型例子就是发生在战国时代的“田忌赛马”故事。

1944 年,美籍匈牙利裔数学家冯·诺依曼和奥地利经济学家摩根斯顿(Oskar Morgenstern,1902—1977)合作发表了长篇巨著《博弈论与经济行为》,标志着现代博弈论的诞生。该书的主要成就包括:

(1)明确了博弈论是一门运用数学方法研究博弈者策略之间相互作用的学科。

(2)提出了“混合策略”的概念,它是通常策略(“纯策略”)的概率组合,此概念揭示了博弈者为迷惑对手以不确定方式出牌的行为;另一方面,所有的混合策略构成了欧氏空间中的“凸集”,从而能够运用无穷小分析和拓扑学等数学工具进行有效处理。

(3)提出了“零和博弈”的概念,即博弈者任何一方所“得”必然会引起其对手之“失”,得失总相等,包括体育竞技在内的大部分博弈都可归结为“零和博弈”。

(4)运用“最小最大准则”①证明了,在两人零和博弈中,存

---

① 该准则设定:博弈者每步行动都是试图从最坏的局面中找出最好的结果来,这个最坏局面是由于其对手在上一步行动中采用同样的准则而造成的。

在一个最优的策略组合，它使博弈者双方均获得最低利益保障：任何一方要偏离此策略，都将减少自己收益并增加对手收益。这一结果被称为“最小最大定理”，是该书的核心内容。

(5)研究了不同情况下的“多人博弈”，特别是有若干参加者结成联盟的多人博弈，得出一些结论，但并没有得到如“两人零和博弈”中那样深刻的定理。



图 1-32　冯·诺依曼



图 1-33　摩根斯顿

凭借冯·诺依曼本人作为 20 世纪最杰出数学家的声望，《博弈论与经济行为》的出版曾在当时引起强烈的反响。人们期望它将把经济学变成像物理学那样的科学，能够用冯·诺依曼提供的数学工具解决其中大部分问题。然而事实是，面对错综复杂的各种经济局面，以“最小最大定理”为核心的博弈论并无多大作为。

兰德(RAND)公司是美国最著名的民间智囊机构，它对博弈论极为推崇。1952—1954 年，兰德公司曾经进行了一系列实验研究，以检验冯·诺依曼的多人博弈理论，结果并没有发现该理论有什么实际作用。

直到另一位传奇数学家——纳什，在不经意之间完成了新

的理论突破，才为博弈论真正开辟了一片广阔的应用新天地。

2. 纯粹数学家的业余爱好

纳什(Jr John Forbes Nash，1928—)出生于美国弗吉尼亚州的布鲁菲尔德，父亲是电气工程师，母亲在结婚前是教师。纳什在宽松的家庭环境中受到良好的教育。上高中时，纳什曾经想成为像父亲那样的电气工程师，但他后来赢得全额奖学金，来到匹兹堡的卡内基技术学院学习化学。因为不喜欢做机械制图和化学定量分析，他又听从了数学老师的建议，改学数学专业。1948 年，纳什以优异的学习成绩，破格同时获得学士和硕士学位，并申请到奖学金，去普林斯顿大学攻读博士学位。



图 1-34　纳什

被誉为当代“世界数学中心”的普林斯顿高级研究所，就坐落在普林斯顿大学中，里面云集了爱因斯坦、哥德尔、外尔、冯・诺依曼等顶级科学大师，更有陈省身、韦伊、谢瓦莱等已崭露头角的数学新杰，经常去那里访问和工作。纳什在这如同天堂般的学术环境中，自由自在地大量汲取数学知识。短短数年中，纳什就在代数几何、微分几何和微分方程这三大数学分支领域中取得重要研究成果，早早奠定了他作为一流数学家的地位。特别是他证明了“任意的黎曼流形都能嵌入欧几里得空间中”，解决了微分几何中一个长期未解决的难题，在数学界引起一片惊奇。

在研究纯数学之余，纳什喜欢思考各种稀奇古怪的问题。例如，他曾发现欧洲有四座城市的位置正好构成一个正方形。纳什对于博弈论更有一种特殊的喜爱。他曾经发明了一些棋类博弈，其中有一种在六边形格子的菱形棋盘上进行，其下法类似于围棋，普林斯顿大学的学生们称它为“纳什棋”。

1949—1953年，纳什发表了4篇关于博弈论的简短论文，改变了博弈论的发展方向。其中一篇论文只有一页长，共28行，却证明了一个极其重要的定理：

在任何一个多人有限博弈中，至少存在这样一个策略组合，使得对于每位博弈者来说，只要其他博弈者都不改变自己的策略，那么他在该组合中的那个策略就是最优策略。

此定理是关于冯·诺依曼两人博弈“最小最大定理”的推广，后来被称为“纳什均衡定理”，而定理中所指的那个策略组合被称为“纳什均衡点”。

另一篇论文研究“多人非合作博弈”，即参加者只考虑各自的利益，彼此之间没有任何同盟关系的博弈，这是冯·诺依曼和摩根斯顿的著作所忽略的。纳什运用他的“均衡定理”，证明了这种博弈至少存在一个“均衡点”，并研究了这些均衡点集合所具有的种种性质。

纳什的另两篇论文研究“两人合作非零和博弈”，同样获得了冯·诺依曼和摩根斯顿所没有涉及的重要结果。

由兰德公司的两位数学家首先发现并且广为流传的“囚徒困境”博弈故事，可以用来说明纳什均衡理论中的有关概念。

有两名犯有抢劫罪的囚徒甲和乙，被分开关押。面对警察

的审讯,他们均有两个策略选择:招供和抵赖。于是就产生4种可能的策略组合以及相应的法律惩罚:a. 甲乙均抵赖,结果两人均将获1年监禁;b. 甲抵赖、乙招供,结果甲获3年监禁、乙被释放;c. 甲招供、乙抵赖,结果甲被释放、乙获3年监禁;d. 甲乙均招供,结果两人均获2年监禁。

“囚徒困境”是“两人非零和博弈”。当甲乙之间有攻守同盟,则同时是“合作”博弈,这时纳什均衡点为策略组合a(两人均抵赖);当甲乙之间没有默契,则是“非合作”博弈,这时纳什均衡点为策略组合d(两人均招供)。

由于泽尔滕和豪尔绍尼在1960年代的工作,人们认识到纳什均衡理论的重要性。博弈论实验也表明:虽然一两次尝试不一定正好得到纳什均衡点,但经过策略调整的多次尝试一定会收敛于该点。现在,纳什均衡理论已成为广泛研究经济学和社会学问题的有效工具。人们甚至发现,该理论同样可用于研究生物学竞争。

纳什1950年获博士学位后,于次年受聘到麻省理工学院教数学。1959年因患偏执型精神分裂症而辞职。在以后的20多年里,疾病不时发作。他曾经想建立世界政府,又宣布自己是南极的国王,还要为抵御外星人入侵而募集资金。幸运的是,在家人无限的关爱和照顾下,他的身心后来竟奇迹般地逐渐康复。到了1980年代末,他甚至已能够重新开始研究数学。

1994年,正值冯·诺依曼和摩根斯坦的著作发表50周年之际,纳什、泽尔滕和豪尔绍尼因“在非合作博弈均衡理论中的开拓性贡献”而分享了诺贝尔经济学奖。瑞典皇家科学院的麦乐

(Karl Göran Mäler)教授在授奖发言中对纳什说到:“您的关于非合作博弈均衡的分析以及其他的博弈论研究工作,对于近 20 年经济学理论的发展产生了深远的影响。”

1998 年,美国女作家和记者娜萨(Sylvia Nasar,1947—)出版了纳什的传记著作《美丽心灵》,引起了世人对这位传奇数学家的关注。2001 年,该书被改编成同名电影。2002 年,该电影赢得了美国奥斯卡“最佳影片”奖。

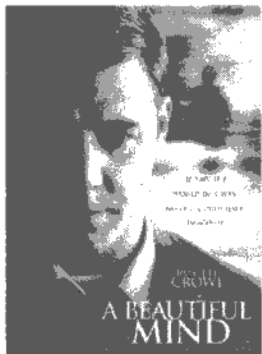


图 1-35　电影《美丽心灵》剧照

3. 纳什工作的进一步研究

与纳什一起获得 1994 年诺贝尔经济学奖的另外两位博弈论专家是泽尔滕和豪尔绍尼。

泽尔滕(Reinhard Selten,1930—)出生于德国的布雷斯劳,在法兰克福大学数学系学习,获得硕士和博士学位。后辗转受聘多所德国大学,任经济学教授。泽尔滕的主要贡献在于完善了纳什均衡理论,并率先研究多阶段动态策略作用。在 1965 年,他首先明确指出,纳什均衡可能由于非理性行为而产生于策略树的不可达处,因而不可解。为消除非理性纳什均衡点,他引进了“子博弈完善”的概念,其要点是排除那些仅仅是口头威胁或讹诈,实际上因代价太大而不可能实施的策略。随后在 1975 年,提出了



图 1-36　泽尔滕

“手颤”的概念，即允许博弈者有发生错误的概率。在以上工作的基础上，他成功建立了寡头垄断市场的模型。麦乐教授在授奖发言中说到：“您的关于完善博弈的分析大大扩展了非合作博弈理论的应用。”

豪尔绍尼(John Charles Harsanyi，1920—2000)出生于匈牙利的布达佩斯，中学时代曾获全国数学竞赛第一名。他所就读的路德中学是匈牙利最好的学校，从这里毕业的学生包括冯·诺依曼和数位诺贝尔奖获得者。1951年，豪尔绍尼和女友设法逃往澳大利亚，又辗转到美国，在斯坦福大学师从著名数理经济学者阿罗攻读经济学博士学位。后长期担任加利福尼亚大学贝克莱分校商学院经济学教授，直至1990年退休。



图 1-37　豪尔绍尼

豪尔绍尼的功绩在于，找到了处理不完全信息博弈的方法，从而确保纳什均衡理论能够用于解决大量的实际问题。

在一场博弈中，如果能够了解到所有参加者的全部信息，就称为“完全信息博弈”，否则就称为“不完全信息博弈”。纳什均衡理论是建立在完全信息博弈的假设基础上的。在现实中，棋类比赛等体育竞技属于完全信息博弈。但在经济和军事等领域，由于公司和军事部门采取保密措施，因此几乎都是不完全信息博弈，这就限制了纳什均衡理论的应用。

1965—1969年，豪尔绍尼受雇于美国军备控制与裁军署，成为10人博弈论专家小组中的成员。博弈论专家们发现，他们无

法给美国与苏联的裁军谈判提供有益的建议和帮助，因为这是一场不完全信息博弈：他们不了解苏联真正的军事实力和政治意图。于是，豪尔绍尼试图解决这一难题。他通过假设信息不完全的博弈者有不确定的几种类型，成功地把不完全信息博弈转换成完全信息博弈。这样，专家们就能够将纳什均衡理论运用于裁军谈判了。

豪尔绍尼的工作使纳什均衡理论有了更广泛的实用性，特别是在经济领域。麦乐教授在授奖发言中说到："您的关于不完全信息博弈的分析，对于信息经济学极为重要。"

未来之舟

2005 年度诺贝尔经济学奖再次授予博弈论学者，他们是以色列耶路撒冷希伯来大学经济学教授奥曼（Robert J Aumann，1930—）和美国马里兰大学荣誉经济学教授谢林（Thomas C Schelling，1921—），因"以博弈论分析方法增进了我们对于冲突与合作的理解"而获奖。还有一些诺贝尔经济学奖获得者的工作也与博弈论有一定的联系。正如诺贝尔奖委员会的网上的新闻公告所说：博弈论已经成为研究经济问题的主要工具。

2

纯粹数学之瑰宝

数学是人类文明的火车头。从埃及、巴比伦、古希腊到东方的阿拉伯、印度、中国，数学不断地引领着科学的进步。以牛顿、莱布尼茨创立微积分为契机，开创了科学的黄金时代，使得世界数学的中心一直在欧洲，20 世纪以后则包括美国。当代的纯粹数学，保持着古希腊数学的优秀传统，同时吸取世界各国数学文化的长处，继续绽放出美丽的花朵，成为人类理性精神的楷模。

2.1 五千年数学发展梗概

本节试图描绘五千年数学发展之概貌，以帮助读者更好地理解本书的全部内容。

1. 数学的起源

史料与研究揭示，人类在 1 万年前的新石器时代已经掌握

了计数和识别一些几何图形的本领。但是直到大约五千年前才开始产生真正的数学。这时人类进入了农业社会，发明了文字，建立了国家：农业要求准确地掌握时令、丈量土地、兴修水利；国家则要进行复杂的商品交换、财富分配和税负摊派；这些都需要数学。而文字使数学知识得以交流和积累。

最早形成的是以测量为主的几何学，值得注意的是它与水患密切相关。埃及的几何学起源于尼罗河泛滥后土地的重新测量，那些测量人被称为拉绳者(图 2-1)。由于尼罗河很久以来每到一年中的 6 月至 10 月就要泛滥，所以要年复一年地在平面土地上用拉绳进行测量，很自然会对几何图形中点、线、面的一般性质和关系有较多的了解和研究。埃及的几何学后来传到希腊，后者结合他们发达的逻辑学，创立了公理化的欧几里得几何学。



图 2-1　古埃及的“拉绳者”，他们是几何学的先驱

在中国，据《史记》和《周髀算经》记载：大禹治水(约4 000年前)，左手拿准绳，右手持规矩，作深、高、远的测量，因而产生了勾股术。大禹治水仅用了 13 年，消除洪患后的田地可以长期保持规则的形状(如象形字“田”所示)，于是计算基本图形(如矩

形、方体和圆）及其截切图形的几何量（如边长、面积或体积）成为中国几何学的主要课题；勾股术则发展成为完整的直角三角形相似理论。在古代中国，数学家被称作“畴人”。



图 2-2　西汉壁画中，伏羲手持矩，女娲手持规，矩用于量直角和画矩形，规用于作圆

此外，建造陵墓（如埃及金字塔）和祭坛（如印度和希腊）也是几何学的重要来源。

代数起源于用加、减、乘、除和开方解决实际应用问题，如几何量的计算、天文测量、实物分配和纯数量的确定等，其中关于平面直边图形和空间直方图形中各种关系量的计算占据着中心的地位。在已发现的，属于4 000年前巴比伦的楔形文字泥石板上，记载着大量的诸如矩形的边长和面积之间关系的代数问题，其解法与现代解一元二次方程的方法一致。

在中国，三国时期的赵爽（约公元 200 年）为《周髀算经》作注中，给出了直角三角形的三边勾股弦之间的一系列的代数关系。在古希腊，欧几里得的《几何原本》（约公元前 300 年）第二卷中内容，实际上就是用几何学的语言叙述代数。而丢番图的《算术》（约公元 250 年）被认为是古希腊代数学的最高成就，其中把数自乘称为“平方”、自乘两次称为“立方”的叫法流传至今。

代数对于几何的依附是长期的，第一部《代数学》的作者阿拉伯学者花拉子米(约 780—850)仍然在用几何方法来证明他的代数结果。直到 19 世纪代数学才完全摆脱现实世界的限制，成长为一门完全独立的学科。

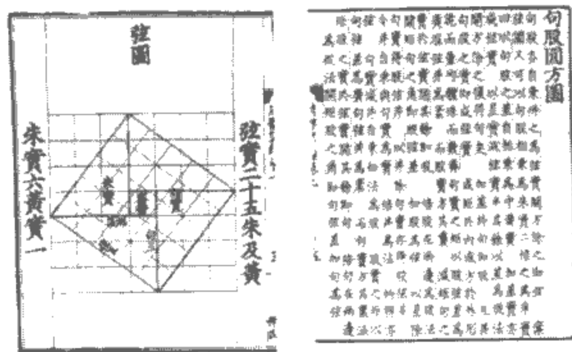


图 2-3 《周髀算经》

计算圆、球以及它们的各种截切图形或生成图形的有关几何量(如圆周率、球表面积、球体积和圆锥体体积等)，在古代数学研究中一直占据重要地位。各大文明中都有最杰出的数学家为之作出贡献：如希腊的欧多克斯(Eudoxus，约公元前 400 年)、阿基米德(Archimedes，约公元前 287—公元前 212)，中国的刘徽(3 世纪)、祖冲之(429—500)和祖暅(6 世纪)，印度的婆什迦罗(1114—1185)，以及日本的关孝和(1637—1708)等。这类计算或明或暗地使用了无限分割的概念，实是 17 世纪后迅速发展的以微积分理论为核心的分析学之滥觞。

古希腊数学闪烁着人类理性的光芒。《几何原本》是人类印刷品中数量仅次于《圣经》的作品。阿基米德留下了大量精彩绝伦的数学珍品。圆锥曲线理论是希腊人独一无二的创造，它起

源于对著名的三大几何问题——化圆为方、倍立方和三等分任意角——的研究。阿波罗尼奥斯(Apollonius,约公元前 262—公元前 190)的《圆锥曲线论》与欧几里得的《几何原本》一样,集中了希腊数学的精华。令人惊奇的是,2 000年后德国天文学家开普勒(Johannes Kepler,1571—1630)发现行星运行的轨道就是以太阳为焦点的一个椭圆! 这导致牛顿发现了万有引力。

几何、代数和分析这三大数学学科,不约而同地产生于各大文明中,虽然具体内容有或多或少的差别。这三门学科刚开始时纠缠在一起,难分彼此;但后来逐渐分离,各自发展成为独立的数学分支。5 000 年来数学经历了千变万化,几何、代数和分析的发展与相互作用则是贯穿始终的主旋律。

2. 几何学的发展

文艺复兴以后,几何学发展的一个方向是形数结合:关于平面和立体简单图形的面积、体积的计算早已转化为代数问题。而法国人笛卡尔(René Descartes,1596—1650)和费马(Pierre de Fermat,1601—1665)引进坐标几何后,把整个几何都代数化了:直线和平面被表为线性代数方程,圆锥曲线表为二元二次方程,而计算图形的面积、体积转化为求函数的积分。从此代数学和分析学成为研究几何的主要工具。

几何图形用代数方程、函数映射以及微分方程来表示,结果产生了大量的更一般的图形,为研究这些图形又发展了新的数学分支:利用导数研究图形的切线、曲率等局部性质导致了微分几何学的产生;为研究代数方程的图形而形成了代数几何学,其

中关于一种二元三次方程图形的研究被称为椭圆曲线理论，它在现代数学中的重要性堪比历史上的圆锥曲线。

几何学的另一个发展方向是探索和研究空间的性质，其中最有深远意义的一步是发现非欧几何。《几何原本》中作为第五公设的平行公理长期以来受到怀疑，不断有人试图用其他 9 条公理把它证明出来，却总是徒劳无功。直到 19 世纪匈牙利人波尔约（János Bolyai，1802—1860）、德国人高斯（Carl Friedrich Gauss，1777—1855）和俄国人罗巴切夫斯基（Николай Иванович Лобачевский，1792—1856）各自独立地认识到这样的证明是不可能的，但是只有罗巴切夫斯基勇敢地公开宣布。他们用不同的公理代替平行公理，从而得到非欧几何。

非欧几何的发现表明并不能简单地根据空间的局部性质来判断整个空间究竟如何。德国人黎曼（G. F. B. Riemann，1826—1966）为了探究局部满足欧氏几何的空间可能会有怎样的结构，创立了黎曼几何。它后来成为爱因斯坦广义相对论的基础。

将直观的曲面推广到高维的一般情形产生了流形的概念：在流形上每个局部都等价于欧氏空间，但其整体的结构却千差万别。把欧氏空间中经典的方法和成果推广到可微流形，成为微分几何学的重要课题：外尔特别是嘉当等人提出外微分方法，运用活动标架法引进了联络的概念，使得欧氏空间中的导数和微分推广到微分流形上；韦伊和陈省身等人把经典的高斯-博内定理推广到黎曼流形；为研究流形上的几何结构，陈省身等人发展了纤维丛理论，它后来被发现与物理学的规范场论不谋而合。

通过考察图形或流形的种种映射性质并结合代数工具对它

们分类，这种研究图形和流形的新方法叫做拓扑学，它由法国人庞加莱(Jules Henri Poincaré，1854—1912)开创。维数、同胚、同伦、同调、连通、亏格等拓扑语言，在 20 世纪的数学文献中随处可见。庞加莱猜想说，单连通的三维闭曲面必与三维球面同胚。这一猜想在 2003 年终于被证明，这是轰动数学界的重大事件。

3. 代数学的发展

在欧洲经历中世纪的漫漫长夜的时候，阿拉伯世界保存和发扬了古希腊数学的传统。花拉子米发明了 algebra(代数学)这个词，其意指“还原”(相当于在等式两边去掉负项)和“对消”(相当于在等式两边消去或合并同类项)；这个词反映了代数的运算特征。而中文译名“代数”为英国来华传教士伟烈亚力(Alexander Wylie，1815—1887)所创，按字面意思可以解释为“(用符号)代替数字(未知量或常量)”，这反映了代数的符号化特征。

代数学在成为一门独立的学科之前，必须走完关键的两步：

第一步是符号化。其中最重要的是未知数的符号化，它的意义在于承认未知数同已知数一样是一种存在的实体，从而可以对它进行运算操作，并研究它的种种性质。在古代中国和日本，曾经发展了一元高次方程的开方术，即求方程根数值解的方法。这些方法并不关心方程根可能有怎样的性质。这是开方术与以后的方程根式解研究的本质区别。

未知数符号化的尝试先后出现在古代的不同国度中。例如，印度人婆罗摩笈多(Brahmagupta，598—665)曾用不同的颜

色表示不同的未知数;在中国宋元时期,李冶(1192—1279)用"天元一"表示一个未知数,而朱世杰(1300前后)则用天、地、人、物四元来表示4个未知数。现代人用字母表示未知数和已知数,并使用"+"、"-"、"×"、"÷"、"="等记号,这些都是在15—17世纪逐步形成的。

第二步是数系的扩展。这涉及运算的封闭性——保证代数方程根的存在。虽然早在2 000年前,中国的《九章算术》中已有完整的分数计算,同时希腊人已经掌握了无理数;但是直到18世纪人们对负数的性质还不甚清楚,并且怀疑复数的存在;一直到该世纪末高斯证明了代数基本定理,人们才接受了研究代数所需要的全部的数(包括复数、四元数和八元数)。复数的价值还在不断呈现,量子力学、电磁学、规范场、复流形等都离不开复数。自此以后,代数学摆脱了对现实世界的依赖,开始了独立的突飞猛进的发展。

代数学发展的一条主线是一元代数方程根式解的研究。虽然早在4 000年前巴比伦人就会用配方法解二次方程,但是直到16世纪意大利的数学家才发现根式解三、四次方程的一般方法。19世纪,阿贝尔(Niels Henrik Abel,1802—1829)证明用根式解一般五次方程不可能。最后是伽罗瓦(Evariste Galois,1811—1832)首创群论方法,确定了n次方程可用根式解的充要条件是其根的置换群为可解群。他在彻底了结这个延续了数千年的代数问题的同时,打开了抽象代数学的发展大门。

抽象代数学研究群、环、域、模、理想、格等代数结构,它在1930年代由诺特与阿廷(Emil Artin,1898—1962)等人正式确

立，成为 20 世纪代数学的主流。

1637 年，费马提出：

> 除平方之外，(正整数)的任何次幂都不可能分拆成两个同次幂。

也就是说，整数解的勾股定理不能向立方以及更高次幂推广，这就是所谓的费马大定理。为证明这个定理，库默(Ernst Eduard Kummer，1810—1893)把整数分解的方法推广到了分圆域，并创立了理想论。他不仅因此发现了“理想”这个新代数结构，而且开创了代数数论的研究。费马大定理最后于 1995 年被英国数学家怀尔斯(Andrew John Wiles，1953—)证明，这是 20 世纪数学最重要成就之一。

“代数”这个词现在不仅代表了一门数学学科，还专指一种带有加法和乘法运算的抽象代数结构。“交换代数”则是研究代数几何的基础。

4. 分析学的发展

17 世纪牛顿和莱布尼茨发明的微积分，被认为“是继欧几里得几何之后，全部数学中最大创造”。其实，它是古代数学中无限分割思想在笛卡尔坐标体系下的自然发展。从此无穷的概念正式进入数学大显身手：无穷小分析成为几乎无处不在的数学语言，无穷级数也被广泛使用。分析学则成为与几何和代数同样重要的数学分支。

函数是分析学的研究对象，极限成为研究函数的基本方法。微分方程、变分法、微分几何等学科不断发展，解决了无数的科

学技术问题,成为人类理解大自然的锐利武器。无穷小理论虽然不严格,却无往不利。200 余年后,分析学的严密化终于获得成功。

法国的傅里叶(Jean Baptiste Joseph Fourier,1768—1830)在研究热传导方程时,将函数展开为三角级数,由此产生了调和分析,并演变为今天的小波分析。

牛顿时代人们只研究光滑的连续函数,但不久就发现了种种不连续、不可微的怪异函数,如何处理这些函数曾使分析学家们伤透脑筋。黎曼曾建立了有限区间上的积分理论,但它不适用于一大类有意义的函数。于是法国人勒贝格(Henri Lebesgue,1875—1941)基于可列可加的测度,创立了关于可测函数的勒贝格积分,由此诞生了实变函数论。

由于研究三角级数收敛点的集合,促使康托(G. F. P. Cantor,1845—1918)创立了集合论,为分析乃至整个数学奠定了逻辑基础。集合论过于宽泛的研究对象,终于出现了悖论,人们曾对集合论是否可靠感到担心。罗素(Betrand Russell,1872—1972)、希尔伯特、布劳威尔等试图为数学建立更牢固的基础,但均未成功。不过,这一悖论虽然是数学大厦基础上的一条裂缝,目前还不会影响整个大厦的牢固存在。

所谓复变函数论实际指单复变量的函数论,它曾经是 19 世纪分析学的中心内容之一:高斯利用它证明了代数基本定理;阿贝尔(Niels Henrik Abel,1802—1829)在这里创造了椭圆函数和椭圆积分;黎曼通过研究多值函数建立了黎曼面理论,这个结构对于几何学和代数学也都有重要意义。整函数与半纯函数的

值分布理论绚丽多彩。多复变函数论则被称为复分析，它形成于 20 世纪初，现在发展十分迅速。基于复数迭代过程而形成的分形理论，别开生面。

研究无限维空间的泛函分析也可称为“函数的”函数理论，因为它研究的是那些作用在函数上的变换或算子。它起源于对变分法和积分方程等的研究。弗雷歇(M. Fréchet，1878—1973)于 1906 年创立了抽象空间(函数是其中的“点”)理论，从而奠定了泛函分析的基础。重要的抽象空间包括巴拿赫空间和希尔伯特空间。泛函分析不仅在数学而且在物理学等学科中有广泛应用，它是现代分析学的基本内容。

5. 纯粹数学与应用数学

数学无疑起源于古人对于现实世界的经验和认识，但经过数千年的曲折发展，它已经成为一门独立于现实世界、具有严密的思想和方法、高度抽象的人类重要知识体系。而在另一方面，数学依然在现实世界以及人类其他的学科领域中有着广泛应用。

于是，形成了两类不同的数学学问：一类致力于研究数学本身的问题，它们被称为“纯粹数学”，也叫“基础数学”，其中主要包括了几何、代数、分析、数论等传统数学以及新兴的拓扑、微分方程和泛函分析等学科；另一类致力于研究数学在其他学科领域中的种种应用，因而被称为“应用数学”。

在 20 世纪，纯粹数学的发展空前繁荣，超过了以往任何时期。但相比之下，由于社会需要和计算机技术的出现，应用数学

所取得的成就更令人印象深刻。在这一时期涌现出大量的应用数学新分支：概率论与数理统计、控制论、信息论、系统论、运筹学、博弈论、分形几何、混沌理论、密码学、计算数学、生物数学、数理经济学，等等。这些新学科不仅为我们提供了观察事物的全新角度和解决问题的有效方法，而且大大加深了我们对整个世界的理解和认识。

纯粹数学与应用数学并非完全分开或相互对立。事实上，在许多应用数学中使用了纯粹数学的工具。而且一些曾经被认为与现实世界没有任何关系、毫无实际使用价值的纯粹数学，也出乎意料地在数学以外找到了用武之地：如抽象代数学和数论用于密码学，微分几何学和拓扑学用于物理学和经济学研究，等等。

6. 21 世纪数学展望

纵观 5 000 年数学，波澜壮阔，精彩缤纷，令人惊叹。浮光掠影地一瞥，当然只能略及皮毛，粗知大概。不过我们还是可以看出，数学的发展与人类文明的进步状况密切相关。

在原始社会，人类只会记数和识别简单的几何图形。这种本领部分出自动物本能的一种发展，部分出自原始部落内部成员间的口头学习和交流。

进入农业社会，人类建立国家，开始了大规模的社会合作、分工和生产。由于社会需要，很自然地产生了以几何学为主干的古典数学。文字著作成为传播数学知识的重要手段，交流的范围也扩大到了整个国家以及属于同一文明的相邻国家。

15世纪开始的欧洲文艺复兴为人类进入工业化社会做准备，数学也开始酝酿思想变革。17世纪以后人类的科学、技术和生产活动越来越广泛深入，数学也随之飞速发展。数学交流使用了杂志论文这种更迅速更方便的手段，并且很快跨越了国界；数学研究已成为国际化的活动。由于人类的这场社会革命首先从西方开始，所以与它同时产生的现代数学也很自然地带上明显的西方古典数学思想的烙印。

21世纪的人类已经跨入了信息时代。计算机和网络使得全球范围的数学交流如同家常便饭；科学技术与生产力水平达到了前所未有的顶峰。在如此环境下，我们可以预料：21世纪的数学将会有远远超过20世纪的大发展，甚至可能会产生新的革命性突破。

中国古代数学曾经在相当长的一段时期内处于世界领先的水平。15世纪以后，由于闭关锁国，中国数学停滞不前，被隔绝于世界数学发展潮流之外。直到20世纪初，落后挨打的中国才开始系统学习和研究现代数学，逐渐缩小了与世界先进水平的差距。新中国实行改革开放之后，中国数学发展更为迅速。2002年，中国在北京首次主办国际数学家大会，表明她已经是一个具有相当国际地位的数学大国。我们坚信，在21世纪，中国将进一步向数学强国的方向迈进。

2.2 从三角形到流形

——认识高斯-博内-陈省身定理

中国古代数学从14世纪开始渐渐落伍。1919年五四运动

以后的现代数学，是学习西方数学、重起炉灶发展起来的。1930年代，中国的两个年轻数学家迅速崛起，介入世界数学的潮流，作出了独特的贡献。一位是华罗庚(1910—1985)，他创立了中国的解析数论学派，并在代数、几何、分析等方面都有出色的工作，成为中国青年的科学偶像。另一位是陈省身(1911—2004)，他受教育于南开、清华、德国汉堡，然后在美国发展，创立了整体微分几何学。1943年，正是战火纷飞的二战年代，陈省身在美国普林斯顿完成了高维高斯-博内定理的内蕴证明，这标志着一个新时代的开始。这一节让我们来认识这一重要定理的科学价值。

1. 从三角形的外角和开始

我们在中学课堂上已经学过平面几何的一个基本定理：

三角形的内角之和等于 π。

其实，此定理还可以等价地表达为：

三角形的外角之和等于 2π。

这样表达的好处是，它对于 $n(\geqslant 3)$ 边形同样成立。用代数符号来表示，就是

$$\sum_{i=1}^{n} a_i = 2\pi, \tag{1}$$

其中 $\sum_{i=1}^{n}$ 表示对1到 n 个加项求和，而加项 a_i 表示第 i 个外角值(图2-4)。

取正 n 边形，并令 $n\to\infty$，则可将式(1)推广到平面圆上。不

过，此时需要使用**微积分学**中的积分表达式：

$$\int_C k \cdot \mathrm{d}l = 2\pi。\tag{2}$$

其中，$\int_C$ 表示在圆周 C 上的积分（即无穷项求和）；k 表示在圆周任一点上的曲率，它是圆半径的倒数；$\mathrm{d}l$ 表示圆周上的微分（即无穷小）线元。式(2)其实对平面上任意曲边形都成立（图 2-4）。

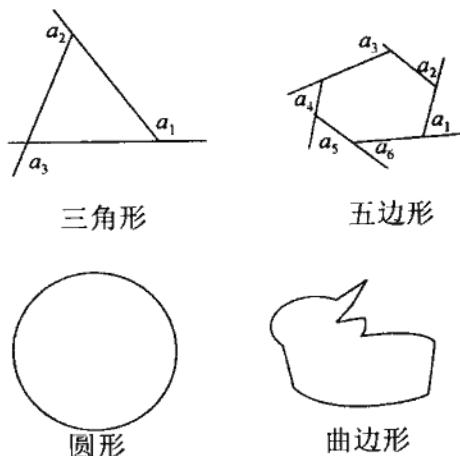


图 2-4

公式(1)和(2)的意义不仅在于给出了一般多边形和一般曲边形的统一表达式，还在于刻画了欧几里得平面的基本性质，即它们与欧几里得的**第五公设**（平行公理）是等价的。

19 世纪发现了两种非欧几何：**椭圆式非欧几何**与**双曲式非欧几何**。要使上述两式在这两种几何中保持成立，必须相应地增加或减去多（曲）边形的面积项。

以上结果很容易推广到三维以及更高维的欧氏或非欧空间。

2. 曲面的高斯曲率

德国人高斯(Johann Carl Friedrich Gauss,1777—1855)被公认是人类有史以来三位最伟大的数学家之一,他在几何、代数、分析、数论等几乎所有的数学主要分支领域都有开创性工作,同时对于物理学、天文学和大地测量学的研究也作出重要贡献。作为非欧几何的发现者之一,他曾主持测量了由三座山峰连接而成的三角形的内角,以弄清现实的物理空间究竟是欧氏空间还是非欧空间。

1827 年 10 月,高斯向格丁廷根皇家学会递交了一篇用拉丁文写就的论文,题目叫做“关于曲面一般研究”,它是开创现代微分几何学研究的经典文献。

高斯在这里首创研究曲面的“内蕴”结构,即与曲面在三维欧氏空间中位置无关的那些性质。这相当于把曲面本身看做是一个“弯曲”的二维空间:在这种空间里,欧几里得的平行公理不一定成立;而且两点之间的最短线也不一定是直线。例如,球面作为一个二维空间,与它是否嵌在三维或高维的其他空间无关。其上两点之间的最短线是大圆。

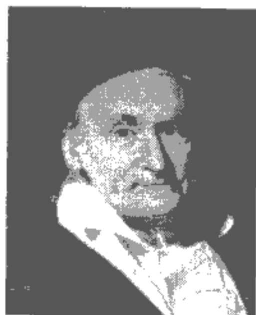


图 2-5 高斯

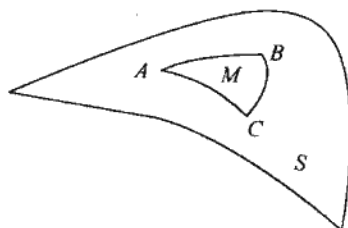


图 2-6 曲面上的三角形图形

高斯定义了一种曲面曲率 k(现在被称作“全曲率”或“高斯曲率”),并证明它是“内蕴的”。接着他证明了他声称是“曲面论中最优美的定理”:对于曲面上用三个点之间的最短线连接起来的“三角形”,其高斯曲率 k 的面积分等于三内角之和与 π 的差。用公式符号表示:

$$\int_M k \cdot \mathrm{d}\sigma = A + B + C - \pi, \tag{3}$$

其中,M 表示曲面 S 上的三角形,$\mathrm{d}\sigma$ 是 M 的微分面积元(图 2-6)。当曲面退化为平面时,$k=0$,于是得到平面三角形的三个内角之和等于 π。这就是前述欧氏平面上的三角形基本定理。当曲面是一个半径为 R 的球面时,$k=1/R^2$;如果取以球心为原点的三根互相垂直的半轴与球面的三个交点,则它们之间的最短线分别在三个互相垂直的大圆上;此时式(3)左边的积分为:球面积$/(8R^2)=\pi/2=$右式。

如同上一节的做法,等式(3)的右边也可以改写成 2π 减去三角形的外角和,于是很自然地把定理推广到曲面多边形的情形。1848 年,法国数学家博内(Pierre Ossian Bonnet,1819—1892)又把它推广到曲边形即闭曲线所围的单连通区域上,这就是著名的高斯-博内公式,它对于曲面几何的重要性就相当于平行公理对于平面几何。其表达公式如下:

$$\int_M k \cdot \mathrm{d}\sigma + \int_C k \cdot \mathrm{d}l = 2\pi\chi(M), \tag{4}$$

其中,C 表示曲边形 M 的边界;$\chi(M)$ 是 M 的欧拉示性数,这是一个拓扑不变量。如果令 g 是曲面上洞眼的个数(比如球面没有洞,故 $g=0$;又如环面有一个洞,故 $g=1$),那么 $\chi(M)=2-$

$2g$。g 也是拓扑不变量，称为曲面的亏格。

当曲面退化为平面时，它的高斯曲率为 0，式(4)就退化为式(2)。当曲面是一个紧致的闭曲面时，就可以对整个曲面进行积分，这时式(4)中左边第 2 项为 0，变成

$$\int_M k\,\mathrm{d}\sigma = 2\pi\chi(M)。 \tag{5}$$

这其实是曲面高斯-博内公式的最常用的形式，其重要意义在于，等式的左面由曲面上各点的二阶导数表示的高斯曲率 k，乃是曲面的局部内蕴性质，而等式右面是表示这一曲面的整体拓扑性质的欧拉示性数 χ，局部与整体的有机结合，体现了数学的核心价值。

3. 黎曼流形

德国人黎曼(Georg Friedrich Bernhard Riemann，1826—1866)是高斯的学生，他堪称是 19 世纪最富有才智和创造力的数学家。现代数学这座大厦中，到处打有黎曼的印记："黎曼积分"、"黎曼面"、"黎曼流形"；关于"黎曼 ζ-函数"零点分布的"黎曼猜想"则是迄今为止尚未解决的最重要的数学猜想。



图 2-7　黎曼

1854 年，黎曼在格丁根大学发表了讲师职位的就职演讲"论几何学基础之假设"，这是现代微分几何学的另一篇奠基性论文。

黎曼在这里把上述高斯的工作，一下子从二维曲面推广到 n

维流形——即那些局部地同构于n维欧氏空间，整体却千差万别的几何结构。

为了通过研究流形的局部性质来了解它的整体性质，黎曼坚持使用高斯所提供的“内蕴”方法。他把欧氏空间中的直线距离的概念作了推广，获得了带有“内蕴的”距离度量的流形，后来被称为“黎曼流形”。

从二维曲面到n维流形，结构复杂性与研究难度同时大大地增加。在相当长的一段时间内，人们都不理解“黎曼流形”，也不知道它有什么用处。直到1913年，爱因斯坦发表了广义相对论(参见1.4节)，人们才发现，黎曼流形比欧氏空间更准确地描述了我们的宇宙。数学家们于是开始深入研究黎曼流形，其中心任务就是要把高斯-博内公式推广到它上面；因为如果能确立此公式，那就像平面几何中有了平行公理一样，流形上的其他问题都能迎刃而解。但这是一个极其困难的任务，耗尽了无数一流数学家的才智。刚开始的时候，人们甚至不知道黎曼流形上的高斯-博内公式应该如何表示。

在以后的30年中，先后通过霍普夫、霍太林、外尔、艾伦多弗和韦伊等人的出色工作，人们终于找到了黎曼流形上高斯曲率的正确表达形式以及相应的高斯-博内公式，并通过把黎曼流形嵌入到高维欧氏空间中的方法，证明了此公式的正确性。但是，当时人们并不知道是否所有的黎曼流形都能够嵌入欧氏空间中①。而且，这种证明方法不是“内蕴”的，有违高斯和黎曼所

① 这一问题在1956年被纳什解决，参见本书1.9节中有关内容。

坚持的研究原则。

4. 陈省身的内蕴证明

1944 年，正在美国普林斯顿高级研究所访问的中国年轻数学家陈省身发表了一篇轰动数学界的论文，题名为“闭黎曼流形高斯-博内公式的一个简单的内蕴证明”。

在短短的不到 6 页纸的篇幅中，陈省身运用嘉当首创的**外微分**方法，对流形上的每一点 P 给出一组正交的单位切向量，称为标架，这些标架与流形本身一起组成了该流形的**单位切丛**。通过反映这些切向量的列维-齐维塔联络性质的方程组，得到关于流形曲率性质的一些外二次微分式，这些微分式的组合得到一个内蕴的 n 阶微分式 Ω，证明这个 Ω 是单位切丛里的一个外导数，然后利用欧拉-庞加莱-霍普夫定理，最后证明关于 Ω 的积分就等于流形的欧拉-庞加莱示性数 χ，这就是高斯-博内公式。



图 2-8　陈省身 1934 年在清华大学读研究生时的照片

陈省身的工作一举解决了这个极其困难又极为关键的几何学问题。但其意义远不止于此。更重要的是，他同时创造了研究整体微分几何(又称“大范围微分几何”)的崭新方法。从此以后，“外微分”、“联络”、“标架”、“丛”成为微分几何的标准术语。

1945 年，陈省身应邀在美国数学会夏季大会上作了“大范围微分几何若干新观点”的演讲，系统阐述了他所发展的纤维丛理

论和外微分方法。大几何学家霍普夫(Heinz Hopf,1894—1971)称赞该演讲标志着“大范围微分几何的新时代开始了”。

同年10月,陈省身又发表了“埃尔米特流形的示性类”论文,其中引进了复流形上一种新的示性类,它后来被称为“陈类”,这是在现代数学中有着广泛应用的一种基本不变量。陈省身由于以上重要的成就,奠定了他在国际数学界中的地位。

著名物理学家杨振宁曾经为陈省身赋诗:

……

造化爱几何,四力纤维能;

千古寸心事,欧高黎嘉陈。

意谓陈省身所创的纤维丛理论将能够统一电磁力、弱力、强力和引力这宇宙四大作用力;并把陈省身与欧几里得、高斯、黎曼和嘉当这些历史上最伟大的几何学家并列。

5. 大师之路

陈省身先生1911年10月28日生于浙江的嘉兴城中,那年发生了推翻两千余年封建帝制的辛亥革命。以后的数十年中,中国经历战乱和动荡;而陈省身的一生却相对比较平稳:少年时就显示了数学的天赋;1926年跳级考入天津南开大学;1934年清华大学算学所研究生毕业;以后虽然经常辗转于世界各地,却再没有离开大学、研究所和他喜爱的数学。

1934年获中华基金会资助,赴德国汉堡大学,师从布拉施克(Wilhelm Johann Eugen Blasschke,1885—1962)研究几何,两年后获博士学位;又赴法国巴黎大学,追随嘉当学习一年,数学功

力突飞猛进。1937 年回国，正值抗日战争爆发，任西南联大数学教授。1943—1946 年在美国的普林斯顿高级研究所访学，期间做出了他最得意的数学工作："开创了整体微分几何的新时代"。

1946 年回到中国后，负责"中央研究院"数学所筹备工作，后任代理所长。1948 年末，国民党政府行将垮台之际，当时的普林斯顿高级研究所所长、美国的原子弹之父奥本海默和维布伦、外尔等大数学家，想方设法把陈省身接到美国。此后他在美国一住 50 年，先后在芝加哥大学、加州大学贝克利分校执教，担任美国数学研究所首任所长，领导了几何学在美国的复兴。

冷战时期中美对立，两国之间几乎割断一切联系。然而陈省身和其他海外华人学者一样，一直对祖国怀着一颗赤子之心。1972 年中美关系解冻，他立即偕夫人和女儿访问阔别了 24 年的祖国。1978 年中国开始改革开放后，他几乎每年来中国，帮助举办学术会议和培养年轻数学家。他提出"中国要在 21 世纪成为数学大国"，这后来被称为"陈省身猜想"。1981 年起，帮助筹备在母校南开大学建立的数学研究所，并成为首任所长。他动情地说："我的最后事业在中国。"表示要为南开数学所的发展"鞠躬尽瘁，死而后已"。他这样说，也确实这样做了。2000 年，他正式回国定居。2002 年，由他和丘成桐倡议的北京国际数学家大会如期召开，陈省身任大会名誉主席。2004 年 12 月 3 日陈省身因心肌梗塞辞世。

陈省身因对微分几何的杰出贡献，1984 年获得被认为是数学最高奖之一的沃尔夫奖，2002 年获几何学最高奖罗巴切夫斯基奖，2004 年获"东方诺贝尔奖"邵逸夫数学奖；还曾荣获美国国

家科学奖章、斯蒂尔奖等。他是包括中国、美国、俄罗斯、英国、法国在内的多个国家的科学院院士。

未来之舟

微分几何学最重要的应用是在理论物理学(参见 1.4 节与 2.3 节);在经济学中也有应用(参见 1.5 节)。与此同时,它在其他数学领域中有广泛应用,如拓扑学、代数几何、复分析、算子代数、微分方程等,都离不开微分几何的概念和方法。

2.3 杨-米尔斯场

——从理论物理到纯粹数学

在当代的数学和物理学研究前沿,二者的关系密不可分。黎曼几何先于相对论,为表达相对论而用,反过来,相对论的出现,推动了微分几何的发展。李群和纤维丛理论先于规范场,为杨-米尔斯规范场所用,反过来,杨-米尔斯方程又推动了当代数学的发展。

1. 数学的相对独立性

毫无疑问,数学起源于人类对于现实世界的实践和认识。然而,数学一旦成为一门独立的学科,就开始按照自身的规律发展,相对地摆脱现实的束缚,最后变成了数学家自由心灵的创造物。许多数学家并不在乎数学有任何的实际用途。19 世纪德国数学家雅可比(Carl Jacobi,1804—1851)曾经说:“科学的唯一目的是为了人类心智的荣耀。在此意义下,一个关于数的问题与一个关于宇宙体系的问题具有同等价值。”

例如，数学家发明了复数和任意维数的空间；虽然现实中并不存在复数，而且我们生活的空间只有三维。美国波兰裔数学家艾伦伯格(Samuel Eilenberg，1913—1998)曾经把自己比作裁缝："有时我做一件五个袖子的外衣，有时做一件七个袖子的；我高兴的时候也做两个袖子的外衣；如果碰巧有人穿我做的外衣正合适，我会很乐意给他穿。"不过，这种摆脱现实世界的自由创造，只能是相对的。当今许多按照"唯美主义"创作出来的数学论文，往往并没有在历史上留下痕迹。就拿四元数和八元数来说，许多数学家期望他们会像复数一样得到广泛应用，但目前还没有。

另一方面，令人惊奇的是，看似数学家脱离现实而自由创造出来的一些纯粹的数学，却能够极其有效地解决现实世界中的各种问题，可以准确地描述隐藏在自然界背后的深刻规律。正如诺贝尔物理学奖获得者威格纳(Eugene Paul Wigner，1902—1995)曾经说过的，"数学在自然科学领域中有着不可思议的效用"。关于数学的这种现象，在物理学中表现得尤为突出。以下是一个经典例子。

中学生都学过椭圆、双曲线和抛物线——它们被称为圆锥曲线，因为都可以通过平面相截于圆锥体获得。圆锥曲线是两千多年前古希腊人独一无二的创造，它起源于对著名的三大几何问题——化圆为方、倍立方和三等分任意角——的研究，因而与宇宙规律并没有什么联系。古希腊数


图 2-9　阿波罗尼奥斯

学家阿波罗尼奥斯所著的《圆锥曲线论》与欧几里得的《几何原本》一样，集中了希腊数学的精华。令人不可思议的是，2 000年后德国物理学家开普勒(Johannes Kepler，1571—1630)发现行星运行的轨道就是以太阳为焦点的椭圆！这后来又导致牛顿发现了万有引力。科学史上一个有趣的问题是，如果没有希腊人的圆锥曲线理论，人类是否还能够发现万有引力？是否还会产生现代科学和现代文明？

前已提及，黎曼肯定没有料到，他出于纯粹的数学理念而创造出来的几何理论，竟能够被爱因斯坦用来刻画真实的物理空间。爱因斯坦以后，数学给物理学家带来惊喜的场面依然不断出现。不仅如此，物理学的进展竟然也同样能够为数学家提供崭新的工具和理念，从而导致数学研究的突破。

2. 陈省身和杨振宁摸到的是同一头大象

在20世纪，数学与物理学频频出演奇妙的双人舞。其中，两位华裔科学家——数学家陈省身和物理学家杨振宁——扮演了中心角色。陈省身和杨振宁(1922—)可谓世交。陈省身曾经与杨振宁的父亲杨武之(1886—1973)一起在清华大学算学系执教。杨老先生还牵线做媒，成全了陈先生的美满婚姻。而杨振宁则在西南联大念书时，听过陈省身的课。

杨振宁于1946年赴美国求学。1954年与米尔斯(Robert L. Mills，1927—1999)合作发表论文，创立了**非交换规范场**理论。1956年与李政道(1926—)合作，发表了推翻弱力宇称守恒定律的论文；1957年与李政道同获诺贝尔物理学奖，成为享誉世

界的物理学大师。

陈省身则于1943—1946年，在美国普林斯顿高级研究所做访问学者；因在此期间给出了高斯-博内公式的内蕴证明，发展了纤维丛和联络理论，开创了整体微分几何新时代而赢得世界声誉。陈省身回国后曾负责筹备“中央研究院”数学研究所，致力于培养青年数学家。终因战乱而于1948年底赴美国定居。

陈、杨两家在美国依旧通好。1962年，杨武之赴瑞士日内瓦与杨振宁相聚，陈省身也专程去会面。在那里，他和杨老先生诗词唱和，合影留念。

然而，陈省身和杨振宁却在相当长的时间内，互相不了解对方的工作。这件事并不奇怪，因为数学和物理是两门有着本质区别的科学，而且均为高度专门化的学问，只有经过长期系统的学习和训练才能够很好地掌握它们。

1960年代以后，杨-米尔斯物理规范场的重要性逐渐为人们所认识。大约在1967年，杨振宁在一次讲课中突然发现，规范场的公式和黎曼几何中的公式极为相似，这令他十分惊奇。他想弄清其中的道理，于是开始学微分几何。但是即使像杨振宁那样有很好数学素养的物理学家，要想搞懂微分几何中那一大堆抽象晦涩的符号和概念也绝非易事。杨振宁有一次在国际物理学家会议上开玩笑说：“现在只有两类数学著作。一类是你看完了第一页就不想看下去了；另一类是你看完了第一行就不想看下去了。”此话博得台下听众一片掌声。

1975年，杨振宁邀请同在纽约州立大学石溪分校执教的几何学家、陈省身的学生西蒙斯(James Simons)教授给本校的物

理学家们作关于微分几何的系列演讲。杨振宁在听课中终于弄懂：物理学的规范场正是微分流形纤维丛上的联络！这使他产生触电般的感觉。他后来写道：

> 客观宇宙的奥秘与基于纯粹逻辑和追求优美而发展起来的数学概念竟然完全吻合，那真是令人感到悚然。

那天晚上，杨振宁驱车来到陈省身家，告知说他已经学懂了漂亮的纤维丛理论和深奥的陈省身-韦伊定理。他说："规范场正是纤维丛上的联络……这既使我震惊，也令我迷惑不解，因为你们数学家居然能凭空想象出这些概念。"陈省身当即反对说："不，不！那些概念不是想象出来的。它们是自然而真实的。"

这就是说，他们摸到的是同一头大象的不同部分。由于有了纤维丛理论作为工具，杨-米尔斯规范场的研究局面被进一步打开。一场物理与数学联姻的好戏由此开始。

3. 数学大家阿蒂亚的介入

曾任英国伦敦数学会主席，英国皇家学会会长，并被英国女王册封为爵士的阿蒂亚(Michael Atiyah，1929—)，是当今世界上屈指可数的顶级数学家之一。



图 2-10　阿蒂亚

阿蒂亚 1929 年 4 月 22 日生于伦敦，阿蒂亚的母亲是苏格兰人，而父亲是黎巴嫩籍的阿拉伯作家。1949 年入剑桥三一学院学习，1952 年毕业，1955 年获博士学

位。1969—1972 年任美国普林斯顿高等研究院数学教授。1973 年回牛津任皇家学会研究教授。1990 年回剑桥任三一学院院长。1990—1995 年任皇家学会会长。这是牛顿曾经担任过的两个英国的最高学术荣誉职位。1990 年他任新建牛顿数学科学研究所首任所长。

阿蒂亚的最重大贡献是同辛格在 1963 年证明了指标定理，把拓扑不变量通过解析不变量来表示。它的大意是说：对一个封闭的弯曲空间 M 上的一类微分算子（称为线性椭圆微分算子），可以定义两个整数：一个是用分析办法定义的，称为分析指标，如算子的核与余核；另一个是用拓扑办法定义的，称为拓扑指标，如 M 的亏格 g。阿蒂亚-辛格指标定理可以叙述为：对任何一个线性椭圆微分算子D，下面的公式成立：

算子 D 的核的维数与余核维数之差 $=1-g$。

这就是说，左边是 D 的分析指标，可以等于 D 所作用的流形M 的拓扑指标。本来彼此不相干的两个概念，现在互相连接成一个等式，何等深刻，何等漂亮！

阿蒂亚-辛格的指标定理被认为是 20 世纪数学最重要的成就之一，它一下子把微分方程、微分几何、代数几何和拓扑学等几个不同数学分支中的一些经典不变量联系起来，因而对整个现代数学发展产生了深远影响。其中，陈省身建立的不变量（陈类）是一个核心概念。

1977 年，原本不怎么关注物理学的阿蒂亚却被刊登在《物理评论》1975 年第 12 期上的一篇论文所吸引，该论文的篇名是“不可积相因子概念和规范场的整体公式”，作者是杨振宁和吴大峻

(1933—,哈佛大学物理学教授)。阿蒂亚和他的同行们注意到文中有一张表,其中把十几个物理学规范场论的术语和微分几何纤维丛中的术语一一对应起来。受到启发,他们就把指标定理用于杨-米尔斯规范场方程,结果竟获得了该方程的自对偶解。于是,数学家们开始对杨-米尔斯规范场产生了浓厚的兴趣。阿蒂亚启动的新一轮研究,即规范理论和拓扑与几何关系,导致 20 世纪最后 25 年拓扑及几何和理论物理如量子场论与弦论的奇妙关系的发现,它把拓扑、几何和物理都带到一个全新的境界。

1982 年,英国牛津大学的二年级研究生唐纳森(Simon Donaldson,1957—)跟随其导师阿蒂亚研究杨-米尔斯方程。但他不是在替物理学家解出这个方程,而是要把它作为探索四维流形结构的工具。

流形 M 上任意两个不同的曲面 α 和 β 会有一些孤立的相交点。可以根据 α 和 β 在这些点上切空间的定向而定义一种双线性形式——称为“相交形式”,它是流形 M 的代数不变量。

唐纳森利用四维可定向紧流形 M 上杨-米尔斯方程的自对偶解的性质,证明了:

如果 M 的“相交形式”是正定的,则它一定等价于标准的欧几里得空间。

但可以找到与欧几里得空间“拓扑同胚”的四维流形,它们的“相交形式”不是正定的。于是,唐纳森立即得到这样的结论:四维欧几里得空间可以有不止一个微分结构!

所谓“欧几里得空间”是指那些满足欧几里得平行公理(或者说满足勾股定理)的几何空间。唐纳森的结果在某种意义下说明了,为什么我们所处的宇宙正好是四维的(三维物理空间加一维时间)。因为四维几何具有最复杂的结构,所以能够产生最丰富的物体,包括星球、原子和生物,以及——人类。

按照阿蒂亚的说法:唐纳森的文章“令整个数学界目瞪口呆”。唐纳森因此项杰出工作而荣获1986年的菲尔兹奖章。

物理学的杨-米尔斯规范场竟然成为探索几何学流形结构的理想工具,数学家们不禁对它进一步刮目相看。在国际数学界,很快形成了杨-米尔斯方程的研究热,并且持久不衰。

4. 西蒙斯:数学家兼金融家



图 2-11　西蒙斯

西蒙斯(James Harris Simons,1938—)堪称是现代数学史上绝无仅有的另类传奇人物。这位鞋厂老板的儿子于1958年从马萨诸塞理工学院(MIT)数学系本科毕业,1962年获加利福尼亚大学贝克莱分校的数学博士学位。1964—1968年在美国国防部所属的国防研究所,从事密码破译工作。因反对越南战争而被解职。1968年起担任纽约州立大学石溪分校数学系主任;而杨振宁则在该校长期担任物理研究所所长。于是就发生了后者请西蒙斯为物理学家讲授纤维丛理论的那段故事。1976年,西蒙斯因在示性形式和极小曲面领域获重要研究成果而与瑟斯顿分享美国数学会颁发的维布

伦几何奖。

1978 年，正当数学事业如日中天的西蒙斯突然辞职，“下海”搞金融投资赚大钱去了。1982 年，他创办了“复兴技术公司”。这家私人投资公司目前经营着世界上最成功的“对冲基金”，其年均投资回报率高达 35% 以上，是对冲基金“大鳄”索罗斯 (George Soros，1930—) 的两倍。索罗斯曾因搞垮墨西哥和英国银行、掀起东南亚金融风暴而名声昭著。西蒙斯和他的公司却极为低调，所以在相当长时间内不为外界所知。而且西蒙斯很少与金融界交往，他几乎不招募经济学或金融专业的毕业生；其公司属下有一个研究部门，里面的员工都拥有数学或物理学博士学位，这些人基本没有金融知识，却建立起极为有效的数学模型和物理学模型来发现证券、期货和货币交易的最优策略。作为对冲基金的管理者，西蒙斯 2005 年的年薪是 15 亿美元，2006 年达 17 亿美元，是全世界唯一的年收入超过 10 亿美元的打工者。

虽然在美国的世界金融交易中心华尔街，西蒙斯并不显山露水，但在国际数学界和物理学界，西蒙斯早已闻名遐迩。而且他的名字总是和另一个名字——陈省身——同时出现。

西蒙斯在 MIT 学习数学时，对微分几何发生了兴趣。他的老师辛格 (Isadore Singer) 告诉他：要想学微分几何，就应该去加利福尼亚大学贝克莱分校找陈省身。西蒙斯于是就来到贝克莱分校数学系读博士。那是在 1959 年，陈省身正好整整一年去欧洲教学访问。西蒙斯于是自学微分几何。每当他学懂一点，就贴海报让大家来听他讲课。真的有不少人去听他的课，其中包

括系里的教授。等陈省身回到贝克莱分校,西蒙斯已经另有导师,但他依然经常找陈省身请教,两人甚至开始合作研究。西蒙斯多年以后回忆到:

> 虽然我并不是如同大家所认为的那样,一开始就跟随陈省身先生做研究。但是我在那里的时候,他经常给我极大的鼓励。当我证明了一个关于极小子簇的定理,打电话告诉他时,他说:"噢!整体的。整体的定理非常好。发现一个漂亮的整体定理总是很难得的。"这对我真是莫大的鼓舞。那一刻,我只想飞快地跑回家,然后证明一百万个整体的定理。在那些年里,我主要研究极小簇,每当我得到一些整体的结果时,我就会打电话告诉陈省身先生:又是一个整体的定理!他总是很高兴地接听我的电话,从电话里,我还能感觉到陈太太也是同样的开心。
>
> 后来当我开始做第二示性类(即现在所称的陈-西蒙斯不变量)的工作时,我把最初得到的一些结果拿去给陈省身看。我很庆幸自己这样做了,因为陈先生了解这些工作更深远的含义。他知道怎样把这一结果推广到高维情形,并且帮助我理解它。我们一起把我的工作所真正蕴涵的内容全部汇集起来,写成了一篇文章。

进入 21 世纪,陈省身回国在天津南开大学定居。西蒙斯曾搭乘私人飞机从美国来天津探望。

西蒙斯所提到的与陈省身合作的论文,于 1974 年发表在美

国《数学纪事》期刊上，题目叫“示性形式与几何不变量”，其中提出了一种新的不变量，后被称为“陈-西蒙斯不变量”。它其实是流形上第二陈类的微分，因而是一个三阶微分形式，其特点是与流形上的度量（对应于物理世界中的“距离”和“长度”概念）无关。谁也没有想到，这个纯粹的几何不变量竟会在 10 多年后与物理学的杨-米尔斯规范场联系起来，并导致产生了一个崭新的物理学领域——拓扑量子场论。而完成这些开创性工作的，是一位横跨数学和物理学领域的大师——威腾。

5. 获得菲尔兹数学奖的物理学家

威腾（Edward Witten，1951—）出生于美国马里兰州巴尔迪摩市的一个犹太人家庭。父亲是物理学家。然而，威腾小时候的理想是要成为一名有资格在著名政治报刊上发文章的记者。1971 年，他获得了布兰达斯大学的历史学和语言学的学士学位；随后考取了威斯康星大学经济系研究生，但只读了一个学期就退学，投入到参议员麦戈文（George Mc-Goven，1922—）的竞选总统活动中。麦戈文后来败给了在任总统尼克松（Richard Nixon，1913—1994）。威腾于是打算回大学继续自己的学业。这次他没有选择文科，而是受父亲的影响，来到普林斯顿大学学习物理，并于 1976 年获物理学博士学位。1976—1980 年，威腾在哈佛大学做博士后。1980 年，他又回到了普林斯顿大学，任物理学教授。



图 2-12　威腾

与其他物理学家的成长经历相比，威腾先文后理，可算是半路出家。这似乎是一个不利条件。但由于曾经受过一些完全不同学科的系统训练，使得他能够从不同的角度来看待物理学问题，反而令他取得了远远高于一般物理学家的成就。

威腾做研究的一大特点是：他善于运用抽象的数学理论来解决物理学难题；同时又反过来，用物理学的概念来解决数学中的难题。

1981 年，威腾取得了第一个重要成就，那就是运用物理学中的超对称概念，给出了关于爱因斯坦方程正质量定理的一个漂亮的简单证明。该定理对于数学家来说是极其困难的，其第一个证明由丘成桐和休恩（Richard Schoen，1950—）于 1979 年给出，这也是使丘成桐获得菲尔兹奖章的一项工作。接着，威腾又成功地把几何学的莫尔斯（Harold Morse，1892—1977）临界点理论和无限维流形上的霍奇-德·拉姆理论，与物理学的超对称量子场论联系起来，进而同时解决了这两大领域中的一系列问题。

1989 年，威腾发表了题目为“量子场论与琼斯多项式”的重要论文。该文把唐纳森处理四维空间杨-米尔斯规范场的方法推广到三维量子场。在这种情况下，威腾创造性地把陈-西蒙斯不变量作用于杨-米尔斯方程，竟然获得了方程的解！须知杨-米尔斯方程其实是一种非线性的偏微分方程，一般情况下很难求出它的解，更不用说在量子场的情况下。而且威腾发现这些解与“琼斯纽结不变量多项式”有密切联系。“琼斯纽结不变量多项式”是新西兰数学家琼斯（Vaugham Frederick Randal Jones，

1952—)在研究算子代数理论中的冯·诺依曼代数的指标定理时发现的。就这样,威腾把这些看似不相干的不同数学领域和不同物理学领域中的理论和概念,全都联系在一起!使人们得以洞察隐藏在这些理论和概念背后的深刻本质!

威腾之所以要在这里使用陈-西蒙斯不变量,因为它是一个与度量无关的三阶微分形式,可以用来获得量子场中一系列与度量无关的拓扑不变量。威腾因此开创了一个崭新的理论——拓扑量子场论。该理论对于物理学和数学都有重要意义。我们知道,牛顿力学和爱因斯坦相对论体系都是一些与空间度量有关的二阶微分方程,这些方程无法用来统一刻画宇宙的四种基本作用力。而陈-西蒙斯不变量与度量无关,因此很可能在一个关于宇宙的统一理论——比如说,弦论——中发挥作用。事实上,威腾的主要研究领域就是弦论。关于威腾的工作,陈省身有专门的评价:

> 威腾是现代最了不起的理论物理学家和数学家……他写的文章对于数学家讲非常难懂,他随便说几句话但没有数学上的严格证明。现在世界上最有名的几何学家、拓扑学家都在拼命读威腾的文章。

一位物理学家竟如此受到全世界数学家的重视,这确实非同寻常。这件事实也说明了物理学和数学之间存在着深刻的联系——诚如陈省身曾经说过的:数学家和物理学家所研究的,只是一头大象的不同部分。

1990 年,威腾"由于把理论物理和现代数学联系起来的工作"而荣获数学家的最高奖——菲尔兹奖章。他是菲尔兹奖章

历史上唯一的物理学家身份的获奖者。阿蒂亚在介绍威腾的获奖工作时说：

> 他的确是一位物理学家，但他对于数学的掌握没有几位数学家能比得上，而且他把物理概念转为数学形式的能力独一无二。他漂亮地运用物理学的洞察力来获得数学深刻的新理论，令数学家不断地感受惊奇……他对现代数学产生了深远的影响。

未来之舟

由于阿蒂亚、唐纳森和威腾等人的工作，使得杨-米尔斯规范场和陈-西蒙斯不变量成为近十几年数学和物理学领域中的热门研究课题。物理学家们还发现，陈-西蒙斯不变量可用于凝聚态物理和超导理论的研究。

目前物理学领域中最引人注目的研究课题"弦论"：该理论认为宇宙是一个 11 维的规范场，而其中所有的基本粒子都是一些或开或闭的"弦"。弦论极有可能克服相对论和量子论的局限，从而给出对宇宙四个基本作用力——引力、电磁力、强力和弱力——的统一的描述。该研究领域的当今领袖人物就是威腾。在弦论中，杨-米尔斯方程、陈-西蒙斯不变量以及卡拉比-丘成桐流形等数学概念均有重要应用。

2.4　从勾股定理到费马大定理

中学生都知道勾股定理。一组整数(3，4，5)能够满足 $x^2+y^2=z^2$。那么是否有一组正整数，能够满足立方和，乃至 N 方和情形？大自然的安排是不可能。

1. 从勾股定理说起

勾股定理断言：

> 任意的直角三角形中，两条直边（勾和股）的平方和等于斜边（弦）的平方。

它是数学中最不同寻常的一条定理。

首先，它是最古老和影响最广泛的定理：4 000 年前的巴比伦人已经知道它；3 000 多年前中国周代人商高也知道它；2 600 年前古希腊人毕达哥拉斯知道并且能够证明它，因此在西方它被称为“毕达哥拉斯定理”。

其次，它是最简单的定理：每个中学生都了解它，并且能够证明它。

最后，它是仅有的、兼具几何和算术意义的基本定理：从几何的角度讲，勾股定理其实与欧几里得平行公理等价，即它们之间可以相互推导。所以在古代中国虽然没有明确使用平行公理，但有了勾股定理也能够解决大量的几何问题。

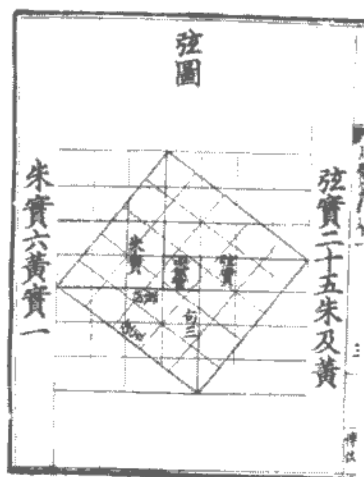


图 2-13　三国时吴人赵爽在《周髀算经》注中，用“弦图”证明勾股定理

从算术的角度讲，勾股定理的不平凡性在于，它存在无穷多个正整数解。“勾三股四弦五”，是其最简单的整数解；其通解是 $a=m^2-n^2, b=2mn, c=m^2+n^2$，其中 m,n 是满足 $m>n$ 的任意正整数。满足勾股定理整数解的三元数组 (a,b,c) 被称为“勾股数”。

17 世纪的法国数学家费马（Pierre de Fermat，1601—1665）在研读古希腊人丢番图的《算术》著作时，看到其中有这样一个关于勾股数的问题：**给定一个整平方数，如何把它写成另两个整平方数之和**？他于是在书的旁边空白处用拉丁文写道：

> 在另一方面，不可能把一个立方整数写成两个立方整数之和，或把一个四次方整数写成两个四次方整数之和；一般来讲，任何一个幂次大于 2 的幂整数都不能写成两个同次幂整数之和。我发现了一个真正奇妙的证明，但空白处太小，写不下。

用代数的语言，费马是在说：

$$x^n + y^n = z^n \quad (n > 2) \tag{1}$$

没有正整数解。

这就是曾经作为数学发展强力助推剂的“费马大定理”。之所以称为“大定理”，是因为还有一个著名的“费马小定理”，这是关于素数性质的重要断言。西方数学家则称之为“费马最后定理”，因为费马曾经有过许多关于整数性质的断言，后来几乎都得到了证明，只剩下这最后一个。

2. 费马的“证明”，只能算猜想

费马究竟有没有证明了他的“大定理”？没有直接肯定或否

定的证据。因为那个时代的数学家大都不主动公布自己的研究成果，而是通过写信，向同行数学家发起解题的挑战，并享受战胜对手的乐趣。不过，现在人们倾向于认为，费马其实并没有真正证明他的定理，因为他不可能掌握那一大堆令人眼花缭乱的抽象数学武器，这些武器都是后代数学英杰为攻克这一难题而专门打造的。



图 2-14　费马

费马曾经写信挑战同行，要求他们证明 $n=3,4$ 时他的“大定理”成立。当然，没有人能够应战。费马本人则在其丢番图《算术》书上的另一空白处，写下了 $n=4$ 时的证明。费马以后的 200 年里，数学家们试图找到对更多 n 的证明，但进展极其缓慢。

18 世纪最伟大的数学家欧拉（Leonhard Euler，1707—1783）只给出了 $n=3$ 时的证明。

19 世纪最伟大的数学家高斯也曾经研究过费马大定理，因得不到结果而放弃。后来他说：

> 我对于费马大定理毫无兴趣，因为这只是一个孤立的命题，我可以很容易地找到一大堆这样的命题，它们既不能被证明又不能被反证。

数学中确实存在许多如高斯所说的“孤立命题”；比如说，断言“在圆周率 π 的十进制数表达中，出现了无限次形如‘0123456789’的数列”就是这样的命题。研究这类命题对于数学的发展并没有什么作用。但是，后来的事实表明，费马大定理的情况完全不是这样的。

所以,当 20 世纪最伟大的数学家希尔伯特被劝说去解决费马大定理时,他说他不愿意杀死这只会下金蛋的鹅。

费马大定理生下了怎样的金蛋?

3. 费马大定理的简单表述引发艰深的“理想”理论

德国数学家库默(Ernst Kummer,1810—1893)迈出了证明费马大定理的关键一步。



图 2-15　库默

我们知道整数有一条基本性质,即

任何整数都能够唯一地分解成不同素数幂的乘积。

如 $20=2^2\times5$,$360=2^3\times3^2\times5$,等等。素数就是那些只能被自己和 1 整除的正整数。

库默首先试图扩大了整数环(记为 $\mathbf{Z}$)的范围,把 n 次单位根(即方程 $x^n-1=0$ 的解,记作 ξ_n)也包括了进去。于是,在扩大的整数环(记为 $\mathbf{Z}(\xi_n)$)中,式(1)就有如此的因式分解(可以假设 n 是奇素数),

$$\begin{aligned} z^n &= x^n + y^n \\ &= (x+y)(x+y\xi_n)(x+y\xi_n^2)\cdots(x+y\xi_n^{n-1})。 \end{aligned} \quad (2)$$

这样,如果 $\mathbf{Z}(\xi_n)$ 依然保持唯一分解的性质,那么费马大定理就能很容易地证明。但遗憾的是,库默很快发现,这种整数环一般不具有唯一分解性质。

非唯一分解整数环的例子可以证明,$\sqrt{-5}\in\mathbf{Z}(\xi_{20})$。于是 6 在这里有两个不同的因子分解,

$$6 = (1+\sqrt{-5})(1-\sqrt{-5}) \text{ 与 } 6 = 2\times 3。$$

为了在扩大的整数环中找到类似于唯一分解整数环的性质，从而能够证明费马大定理，库默创立了一种漂亮的代数理论，叫做“理想论”。这里的“理想”，是指一种带有代数结构的整数集合，其中的元素满足加法封闭性和整数相乘的封闭性。比如说，在标准的整数环 $\mathbf{Z}$ 中，集合

$$I_5 = \{5x \mid x \in \mathbf{Z}\}$$

就是一个理想，它由 5 的所有整数倍组成。这样，所有的整数都能对应于一个理想。反过来，如果是唯一分解整数环，那么所有的理想也正好对应于一个整数（允许相差一个单位因子，如“－1”）；如果不是唯一分解整数环，则存在不能对应于任何整数的理想；但在任何情况下，都可以对理想进行因子分解，就好像整数的因子分解。

库默证明了一个极为精彩的关于理想分解的定理：

> 在代数整数环中，任何理想都能够唯一地分解成不同素理想幂的乘积。

我们看到，这条定理与前面的关于整数唯一分解的性质对应。根据这条定理，那些扩大的整数环 $\mathbf{Z}(\xi_n)$ 虽然一般不具有整数唯一分解性质，但都具有“理想”唯一分解性质。

库默进而把素数分为两类：正则的和非正则的；并证明了正则素数时的费马大定理。这样就一下子得到：除了个别情况，费马大定理当 $n \leqslant 100$ 时成立。

库默的“理想论”堪称是 19 世纪最重要的代数学成就之一。在其基础上，又诞生了分圆域论、代数数论、类域论等一系列 20

世纪代数学热门分支，这些都属于费马大定理所产下的金蛋。

4. 引导纯粹数学进步的一座“金矿”

又过了 100 多年，虽然不时有所进展或突破，但是费马大定理依然没有被完全攻克。数学家开始寻找新的武器，他们把眼光对准了“代数几何”，这是在 20 世纪下半叶中最具活力的纯粹数学新领域。迄今为止，在有“数学诺贝尔奖”之称的菲尔兹奖章获得者的全部 40 余人中，代数几何学家占据了 10 位。

简单地讲，代数几何研究代数方程的图形性质。一次代数方程的图形是直线或平面，二次方程的图形是圆、椭圆、双曲线(面)或抛物线(面)，代数几何主要研究三次及以上的代数方程。其中一个最简单的研究对象就是形如

$$y^2 = Ax^3 + Bx^2 + Cx + D$$

的方程，称作“椭圆曲线”，所以叫此名字是因为它能够被一个“椭圆函数”参数化，“椭圆函数”来源于求椭圆的周长，它是三角函数的推广。

1984 年，德国数学家弗雷(Gerhard Frey，1944—)把费马大定理与椭圆曲线联系起来。他假设“大定理”不成立，即存在 $n>2$和正整数 a,b,c，使得 $a^n+b^n=c^n$。则可以定义一条有理数域上的椭圆曲线：

$$y^2 = x(x-a^n)(x-b^n)。 \tag{3}$$

他猜测这个椭圆曲线具有一些奇怪的性质，因而可能不存在。两年后，美国数学家里贝特(Kenneth Ribet)证实弗雷的猜测，他证明，椭圆曲线(3)的 L-函数并不对应于任何“模形式”。而这一

结论与一个著名的代数几何猜想矛盾：

谷山-志村-韦伊猜想　有理数域上椭圆曲线的 L-函数都对应于一个“模形式”。这里的“对应”，是指 L-函数的展开式与“模形式”的傅里叶级数展开式有着相同的系数项。

数学小知识　有理曲线的“L-函数”由该曲线在每个有限素域中的零点个数组合而成，它是“黎曼 ζ-函数”的一种推广。“模形式”是定义在复数上半平面上的一类解析函数，它在“模群”变换的作用下保持规定的不变性；“模群”就是作用于复数平面上的分式变换，它是一种“李群”。

于是，只要能够证明谷山-志村-韦伊猜想，说明式(3)的椭圆曲线不存在，就证明了费马大定理。

持续了 350 多年的“围剿”费马大定理的战争，进入到最后攻坚阶段。

5. 日本数学家的一个突破

日本自 1868 年“明治维新”后，开始全盘接受西方科学技术与文化，因而领先于中国，较早地进入现代化国家行列。

在数学研究领域，日本同样起步早，进步快。高木贞治(1875—1960)在东京大学毕业后，赴德国哥廷根大学，追随希尔伯特研究代数数论，不久就证明了被称为“克罗内克青春之梦”的有关代数数域性质的猜想，这是日本第一个具有世界水平的数学研究成果；后来又创立了“类域论”，这是关于“理想”分类的代数理论。高木贞治因此成为日本现代数学第一人。在他的影响之下，日本的代数数论和代数几何的研究一直居于世界先进

水平之列。日本迄今为止有三人获得过代表数学家最高荣誉的菲尔兹奖章:小平邦彦(Kodaira Kunihiko,1915—1997)、广中平祐(Hironaka Heisuke,1931—)和森重文(Shigffumi Mori,1951—),他们都是代数几何学家。

年轻的代数几何学家谷山丰(Taniyama Yutaka,1927—1958)是东京大学的教师,他有点懒散,心不在焉,却具有非凡的数学才华。他与志村五郎(Goro Shimura,1930—)合作创立了“阿贝尔簇复乘法理论”。1955年,在东京召开的一次代数数论研讨会上,谷山又提出了“有理数域上每一条椭圆曲线都是模函数域上一个雅可比因子”等猜想。它们后来经志村五郎和韦伊的完善,形成了谷山-志村-韦伊猜想。

1958年11月17日,这位生活美满且前程远大的年轻数学家突然自杀。谷山丰在遗书中写道:“直到昨天我也没有动过自杀的念头。但不少人已注意到我近来身心疲惫。至于自杀的理由,我也不清楚自己究竟为什么,但并非由特别的事件或原因引起……请原谅我最后一次自行其是,我一生总是这样。”1个月后,他的未婚妻铃木美沙子也选择了自杀,她留下遗言:“我们说过永不分离。现在他已走,我也要去和他在一起。”如同樱花绚丽开放后突然凋谢,谷山丰的行为折射出经历二次世界大战战败的日本年青一代对于人生的失落和迷茫的感觉。

6. 最后的冲击

英国人怀尔斯(Andrew Wiles,1953—)在10岁时就已经知道了费马大定理,并且梦想能够证明它,这使他后来选择了数学

家的职业。怀尔斯于 1980 年获得了剑桥大学博士学位，后来到美国普林斯顿大学教数学。在以后几年里，怀尔斯获得了一些重要的研究成果，因而赢得了世界一流代数数论和代数几何专家的声誉。但他所做的这些研究，只是在为冲击费马大定理而锻造武器和练习身手。1986 年，怀尔斯获悉了弗雷和里贝特的工作，他敏锐地感觉到，攻克费马大定理的最佳时机已来到，自己绝不能错过这一机会。他于是马上全力以赴投入到谷山-志村-韦伊猜想的证明中。为了避免干扰，除了新婚不久的妻子，他没有告诉任何人他正在做什么。


图 2-16　怀尔斯

从表面上看，证明谷山-志村-韦伊猜想的难度一点不亚于直接证明费马大定理：它几乎令人无从下手，所以 30 多年来没有人想到要去证明它。凭借学识和经验，怀尔斯决定从比较椭圆曲线和模形式两者的“伽罗瓦群表示”着手。实践证明，这是一条正确的道路。

这样，整整过了 7 年，怀尔斯终于证明了特殊条件下的谷山-志村-韦伊猜想；重要的是，这个特殊条件包含了费马大定理。

1993 年 6 月，怀尔斯在英国剑桥大学牛顿研究所举行主题为“椭圆曲线、模形式与伽罗瓦群表示”的系列学术讲座。在讲座的最后一天，他面对一群数学家平静地宣布，“我已经证明了费马大定理”。随即在听众中爆发出热烈的掌声。这一重大新闻很快传遍了全世界。

然而,现实往往并不那么具有戏剧性。不久发现,怀尔斯的证明中还隐藏着一个不大不小的漏洞。他立即着手修补,但一年很快过去,没有什么进展。怀尔斯有点泄气,想打退堂鼓了。眼看他也要加入"倒霉的费马大定理证明失败者"的庞大队伍中。

在助手的激励下,怀尔斯决定作最后一次尝试。1994 年 9 月 19 日,他突然有灵感——想出了一个绕过漏洞,补全证明的绝妙方法。这一次,他真的成功了。现代数学史上最古老的一个难题,终于被完全破解! 很快,他的 100 多页长的论文被几位国际权威专家审查通过,在一家国际顶级的数学杂志上正式发表。

怀尔斯在接受媒体采访时坦陈,在经过长达八年夜以继日的艰苦工作而取得成功之后,他有着巨大的成就感和精神自由感;同时感到有点忧伤和悲哀:我们从此失去了那件东西,它曾经长期伴随着我们,是我们儿时的梦想,并把我们带进了数学。

1998 年,国际数学联盟破例授予怀尔斯特别奖,以表彰他完全证明了费马大定理的成就,同时补偿他因已超过 40 岁而不能获得菲尔兹奖章的遗憾。此外,怀尔斯还荣获了 1996 年度沃尔夫奖和 2005 年度邵逸夫数学奖,以及其他多项大奖。

未来之舟

费马大定理的被证明,堪称是 20 世纪数学最辉煌的成果之一。然而,其意义远不仅限于解决了一个著名难题。更重要的是,在证明的过程中,产生了一些有生命力的新概念和新方法,并建立了不同领域之间深刻的联系,这将进一步对数学的发展产生深远的影响。1999 年,谷山-志村-韦伊猜想被宣布已完全证明,一些相关的问题也随之一起被解决,所使用的就

是由怀尔斯创立的方法。当然，数学的发展是无止境的。尤其在代数数论和代数几何领域，还有许多重要猜想等待现在和未来的数学家们去证明。

2.5　破解拓扑学世纪之谜：庞加莱猜想的证明历程

进入 21 世纪，纯粹数学的一个重大突破是庞加莱猜想的解决。俄罗斯学者佩雷尔曼的天才创意和拒绝领奖的传奇故事，令人叹服。一批华人学者参与了最后的论证，值得称道。

1. 庞加莱关于“拓扑学”的天才创见

在 19、20 世纪交替之际，没有一位数学家能够预料，甚至希尔伯特在其著名的 23 个问题中也没有任何的暗示，一门崭新的数学分支——拓扑学——很快就要出现，并且将在今后百年中占据纯粹数学的中心舞台。

1904 年，法国人庞加莱（Henri Poincaré，1854—1912），当时唯一能与希尔伯特匹敌的伟大数学家，发表了以“位置分析”为题目的论文，标志着拓扑学的诞生。



图 2-17　庞加莱

拓扑学又被称为“橡胶布几何学”，它研究几何图形在经过放大、缩小或扭曲变形后仍然能够保持的那些整体性质。进入了 20 世纪以后，数学研究的问题越来越复杂，如各种代数方程和微分方程，其中绝大部分已不可能找到精确解。于是数学家开始转向研究由这些方

程所决定的几何图形结构及其分类。拓扑学由此应运而生，成为现代数学的一门“显学”。

庞加莱在他的开创性论文中，提出了这样一个问题：

> 一个闭的三维几何图形，若其上的每条闭曲线都可以连续收缩到一个点，那么从拓扑上来看，这个图形是否一定是球面？

这就是著名的庞加莱猜想，它一直是拓扑学研究的中心课题，曾经顽强地经受了数学家们整整100年的轮番冲击。

庞加莱猜想可以很自然地推广到其他维数。一维的情况是平凡的。二维的几何图形就是曲面，这时相应的猜想也很简单。因为闭曲面的所有分类已经完全搞清，其中“可定向”闭曲面的分类由它们的“亏格”(图形中“孔洞”的个数)唯一确定。如图2-18所示分别是亏格0到2的可定向闭曲面图形。

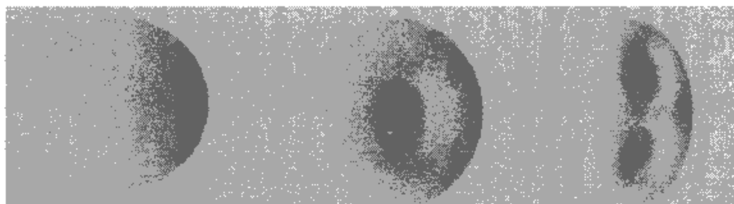


图2-18 可定向闭曲面图形

数学小知识 “定向”是拓扑学的一个基本概念：如果一只想象中的蚂蚁在一个曲面上无论怎样爬行都不会爬到曲面的另一侧，就称该曲面“可定向”；否则，称为“不可定向”。不可定向曲面的最简单例子是“麦比乌斯带”(图2-19)。

不难验证，只有亏格为 0 的曲面满足庞加莱条件，这样的曲面必然拓扑同构于球面，因而庞加莱猜想成立。

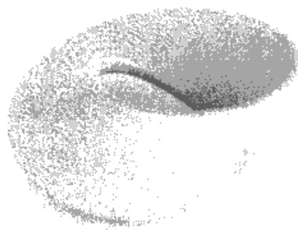


图 2-19 麦比乌斯带

拓扑学的三维球面应该是什么样子？人们很难想象。因为它只存在于四维或更高维的空间中，而现实空间只有长、宽、高三维。但是，如果增加时间这一维，我们还是能够大致描绘它的图形。想象一个二维球面，其半径 R 随着时间 t 变化：$t=0$ 时，$R=0$；接着 R 随 t 一起增大；当 $t=1$，$R=1$，达到最大；接着 R 随 t 增大而减小；当 $t=2$ 时，$R=0$（图 2-20）。这样在时-空坐标系中，就会出现一个三维球面的图形，其代数方程式是

$$x^2+y^2+z^2=1-(t-1)^2。$$

还有一种"内蕴"地看三维球面的方法，就是把它当作微分几何中的流形，此时它等价于我们的三维欧氏空间再加上一个"无穷远点"。

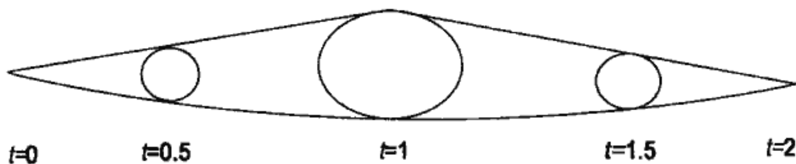


图 2-20

2. 只剩下"三维"情形的硬骨头

令人惊奇的是，对三维以上的几何图形来说，相应的庞加莱

猜想陆续得到证明。只剩下原始的三维情形，困扰着21世纪之交的数学家们。

1960年，美国数学家斯梅尔(Stephen Smale，1930—)一下子证明了五维及五维以上维数图形的广义庞加莱猜想，他因此获得了1966年菲尔兹奖章。

1982年，当时还只是一名研究生的英国数学家唐纳德森(Simon K. Donaldson，1957—)，利用物理学的杨-米尔斯方程，发现了四维空间能够具有不同于欧几里得空间的微分结构；同年，美国数学家弗里德曼(Michael H. Freedman，1951—)利用唐纳德森的结果，证明了四维图形的庞加莱猜想。唐纳德森与弗里德曼因此同获1986年菲尔兹奖章。

于是，只有三维图形的(即原始的)庞加莱猜想尚未被证明。因为这种维数的情况最为复杂(想一想现实的三维世界是多么丰富多彩！)，使得图形的拓扑分类变得极其困难。当然，并非没有任何进展，只是路途还很漫长。

美国几何学家瑟斯顿(William P Thurston，1946—)对于三维图形具有超强的直观能力。1978年，他提出了"所有的三维空间(即几何图形)都可以由8种基本空间合成"的断言，被称为"瑟斯顿几何化猜想"。这8种基本空间包括三维欧氏空间、三维球面、三维双曲型非欧空间以及另外5种有点怪异的黎曼空间。由此容易看出，瑟斯顿的断言蕴含了庞加莱猜想。后来的发展表明，瑟斯顿指示了攻克



图2-21　瑟斯顿

庞加莱猜想的一个正确方向。1982 年，瑟斯顿因其在三维流形研究中开创性的工作而荣获菲尔兹奖章。

3."几何分析"方法另辟蹊径

拓扑学的早期研究主要使用代数方法，因此有"代数拓扑学"之称。后来，微分几何逐渐成为拓扑学的主要研究工具，于是又有"微分拓扑学"之名。

微分几何研究"流形"，或叫做"空间"，其实就是拓扑学中的几何图形。由于高斯、黎曼、嘉当和陈省身等人的开拓性工作，微分几何已发展成为纯粹数学的一个充满活力的主要分支；凭借其处理流形的丰富手段，因而能够在拓扑学研究中发挥强有力的作用。特别是一种叫做"几何分析"的方法，它通过解流形上的非线性偏微分方程来揭示流形的结构信息，后来成为打通庞加莱猜想证明之路的利器。

偏微分方程属于数学的分析领域，将其放在流形上后，就形成了几何与分析交叉的一个新领域，所以称为"几何分析"。该领域兴起于 20 世纪 70 年代，著名华人数学家丘成桐一直是其中的领袖人物。



图 2-22　丘成桐

丘成桐(Shing-Tung Yau，1949—)出生于广东省汕头市，不久移居香港。14 岁时，身为大学哲学教授的父亲突然病逝，使全家生活陷于困境。全凭母亲支撑，将七个子女抚养长大。丘成桐小时侯读书并不用功，父亲过世令他开始发奋；1966 年以优异成绩考入香港

中文大学数学系；三年后来到美国加利福尼亚大学伯克利分校，在陈省身指导下学习微分几何，并于1971年提前获取博士学位。他先后在普林斯顿高等研究所任研究员，在加州大学圣地亚哥大学任教授，1987年起任哈佛大学教授；1993年，在加入美国国籍之后当选为美国科学院院士。

丘成桐的代表性数学贡献就是于1976年证明了“卡拉比猜想”，这是由意大利裔美国几何学家卡拉比（Eugenio Calabi，1924—）在1954年提出的，关于紧复流形上的第一陈（省身）示性类与度量之间关系的一个断言；他的另一个重要贡献是在1978年与人合作证明了广义相对论中的正质量猜测。这些成就大都通过解流形上的偏微分方程取得。

1983年，丘成桐成为第一位荣获菲尔兹奖章的华人数学家。尼伦伯格（Louis Nirenberg，1925—）在介绍其获奖工作时说道：

> 丘成桐在微分几何和偏微分方程领域中做出了极其深刻和极有影响的工作；他是一位兼具强大计算力和洞察力的分析几何学家（或叫做几何分析学家）；他解决了那些多年内未曾有任何进展的难题。

4. 哈密尔顿打下基础

1982年，美国数学家哈密尔顿（Richard Hamilton，1943—）发表了题名“三维流形的里奇曲率”的论文，其中首先引进了“里奇流”的概念。“里奇曲率”是以意大利微分几何学家里奇（Gregorio Ricci-Curbastro，1853—1956）的姓命名的，刻画黎曼流形局部弯曲性质的一个特征变量。“里奇流”则是指定义在黎曼流

形上的一个关于“里奇曲率”的热传导型方程(一种非线性偏微分方程);它会使曲率如同热扩散一样随着时间的增长而逐渐变得各处均匀。



图 2-23　哈密尔顿

丘成桐立即看出,“里奇流”在使流形的形状“变好”的同时,还会因流形的“塌陷”而产生“瓶颈”之类的奇点,从而可以把流形分解成几个较简单的流形的组合,如此分解下去,最后可能得到一些足够简单的流形,从而能够验证“瑟斯顿几何化猜想”(包括庞加莱猜想)。他于是力劝哈密尔顿朝此方向前进,并鼓励自己的学生也积极投入其中。

经过 20 多年的努力,哈密尔顿已澄清了绝大部分奇点的情况。在他的研究中,大量引用了丘成桐、李伟光、施皖雄、曹怀东、朱熹平等华人数学家的成果。现在,只对一类特殊的奇点——雪茄型奇点——不能把握,因为这类奇点可能会使流形的分解无限次进行下去,以至不能产生最简单的流形。

哈密尔顿为证明庞加莱猜想作出了关键的贡献,但因超龄而未能获得菲尔兹奖章。不过,他于 1996 年荣获了美国数学会的维布伦几何学奖,并于 1999 年当选美国科学院院士。

5. 佩雷尔曼立首功却拒绝领奖

从 2002 年 11 月到 2003 年 7 月这短短的半年多时间里,俄罗斯数学家佩雷尔曼连续在因特网上发表了三篇关于“里奇流”的研究论文,引起了国际数学界的震动,因为这些论文的结果如

果是正确的话，那就意味着“瑟斯顿几何化猜想”当然也包括庞加莱猜想被完全证明。佩雷尔曼在他的论文里使用了改进的流形分解方法，并且证明此时不会出现哈密尔顿所担心的那个“雪茄型奇点”。于是，由“里奇流”引起的所有流形分解都将在有限时间内完成；并且已经知道，所得到的最简单流形只能是瑟斯顿所给出的8种基本流形中的一种。就这样，困扰了数学家整整一个世纪的拓扑学之谜被完全破解。

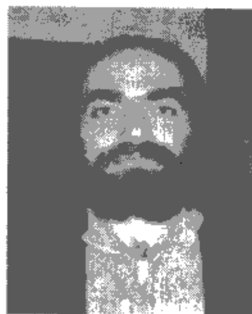


图2-24 佩雷尔曼

然而，佩雷尔曼的论文很简略，许多地方只是梗概地说明。他本人在发表了文章后，曾应邀来到美国的几所大学讲解他的理论。但回到俄国后就马上销声匿迹，不肯露面。人们一时无法确定他的结果是否正确无误，于是数学家们开始设法补全他的证明。经过三年的努力，到了2006年，朱熹平和曹怀东合作的长达592页的论文，田刚和摩根的473页论文，以及克莱恩和洛特的192页论文先后发表。这几位一流数学家的详尽工作得出了相同的结论，即佩雷尔曼的结果是正确的。

在2006年8月召开的国际数学家大会上，国际数学联盟宣布授予佩雷尔曼菲尔兹奖章。这是历史上首次把该奖章授予一位把获奖成果公布在因特网而不是发表在正式杂志上的数学家。更令人意外的是，特立独行的佩雷尔曼拒绝接受这象征数学家无上荣誉的金质奖章。

佩雷尔曼1966年6月13日出生于苏联列宁格勒（现已恢

复旧名圣彼得堡)的一个犹太人家庭;1982 年参加中学生国际数学奥林匹克竞赛,以满分获得金牌;随即进入列宁格勒国立大学学习几何,直到 20 世纪 80 年代末获博士学位;后在著名的斯捷克洛夫数学研究所工作,期间曾赴美国访学;1994 年受邀在苏黎世国际数学家大会上作过报告。

未来之舟

庞加莱猜想的证明是 21 世纪数学取得的第一个重大成果,它将对这一世纪的数学和理论物理学发展产生深远影响。

"里奇曲率"与爱因斯坦的广义相对论有密切关系,因为根据广义相对论,物质的存在将引起空间弯曲。所以,由里奇曲率随时间变化而产生的"里奇流"将成为 21 世纪研究物理空间结构演变的新武器。与此同时,一些类似于里奇流的新概念开始出现,比如说,已经有了"卡拉比流"的研究。在另一方面,"几何分析"方法将继续在微分几何、拓扑学、代数几何以及物理学等领域中发挥重要的作用。事实上,丘成桐在证明"卡拉比猜想"中所研究的那种复流形,已被命名为"卡拉比-丘流形",它正在被物理学的"弦论"用于刻画那个在 11 维的物理世界中被隐藏的"六维空间"。

3

应用数学之精粹

传统的应用数学，总是为“力、热、电、光”等科学技术工程领域提供工具。20世纪以来的应用数学，继承传统，又突破传统，迈进随机数学领域，进入数字时代。信息论、控制论、机器证明、密码学等等，成为一个个单独的数学学科。

3.1　从帕斯卡到柯尔莫哥洛夫
——概率论之发展史

帕斯卡和费马关于赌金的思考，揭开了随机数学的序幕。但是，当确定性数学在18、19世纪大放异彩之时，随机性数学却发展缓慢。1933年，苏联数学家柯尔莫哥洛夫给出概率的公理化定义，概率论终于成为一门严谨的数学学科。

1. 充满随机现象的自然界“确定性”应用数学的作用与局限

18世纪法国数学家拉普拉斯（Pierre-Simon Laplace，

1749—1827)运用牛顿数学，创作了关于宇宙演化的经典巨著《天体力学》(共5卷16册)。当时的法国皇帝拿破仑(Napoleon Bonaparte,1769—1821)问他："你写下这部关于宇宙体系的大作，里面只字不提造物主(上帝)?"拉普拉斯回答说："陛下，我不需要这个假设。"



图 3-1　牛顿



图 3-2　拉普拉斯



图 3-3　儿童时代的麦克斯韦

"确定性"应用数学的另一个重要例子是19世纪英国数学家麦克斯韦(James Clerk Maxwell,1831—1879)所创立的电磁场方程，它给20世纪的人类带来了奇妙的电子时代：电话、电报、电影、收音机、电视机、雷达、激光、光纤、人造卫星以及电灯、电炉、微波炉、电冰箱、空调、洗衣机……当然，还有电子计算机。

其他"确定性"数学的例子还有热传导方程和振动方程等，它们在工程领域有着广泛的应用。

然而到了20世纪，人们发现，牛顿所代表的确定性数学虽然应用极其广泛，其实它们只能够描述一小部分事物和现象，另外还有很大一部分完全不在其把握之中。比如说，它们不能断定任何一次掷骰子将会出现几点；不能确定哪支球队会赢得足球比赛；不知道一个人出门将遇上车祸还是会买到中奖彩票；不能预料股票价格是升还是降；不能预测人的生老病死；无法描述

气体中的分子运动;不能描述电子如何绕原子运动……特别是,人类已进入了信息时代,而确定性数学根本无法说明,信息究竟为何物。

随着文明的发展和科技的进步,人类不得不面对越来越多的“随机性”事件和现象——它们的发生和产生涉及太多或太复杂的因素,所以无法用确定性数学来处理。

通过本书我们将看到:20 世纪发展起来的应用数学大多属于“非确定”数学,即它们所研究的对象大多带有不同程度的“随机性”,因而能够弥补“确定性”数学的不足。而概率论则是直接把“随机性”本身作为研究对象,探索其中“确定性”规律的一门特殊的“非确定”数学,它同时为其他“非确定”数学提供了理论框架和研究手段。

2. 概率论产生于赌金分配

“骰子”下诞生的概率论　赌博是人类固有的恶习,古今中外有多少人沉迷于其中而不能自拔。然而,赌徒们为了赢钱而要钻研骰子点数和纸牌组合的分布规律;后来,数学家也被吸引进来;于是,产生了最早的概率理论。

17 世纪的法国两位天才数学家帕斯卡(Blaise Pascal,1623—1662)和费马(Pierre de Fermat,1601—1665)(还记得“费马大定理”吗?)曾在 1654 年就“赌金分配”问题进行了一系列通信,被认为是近代概率论的肇始。



图 3-4　帕斯卡

事情起因于一位被尊称为"德·梅莱骑士"(Antoine Gombaud,Chevalier de Méré,1607—1684)的法国小贵族。他是作家也是狂热的赌徒,经常设计一些成功几率看似不大、实际稍大于失败几率的赌局,以引诱不知情的人参赌。其中有两种赌局因他而出名:

德·梅莱骑士的赌局 (1)掷一粒骰子4次,要求至少有一次掷出6点;(2)掷两粒骰子24次,要求至少有一次掷出双6点。

德·梅莱认为这两种赌局的获胜几率相同,都稍大于失败几率。其理由是:掷一粒骰子可能出现6种结果,掷两粒骰子可能出现36种结果;因为 $24:36=4:6$,所以它们的获胜几率相同。

然而,当德·梅莱把他的想法告诉帕斯卡,后者用组合方法进行了严格的计算后,却告诉他:这两种赌局的获胜几率不一样!事实上,正确的结果是:第一种赌局的获胜几率稍大于失败几率(比值为 $671:625\approx0.5177:0.4823$);而第二种赌局的获胜几率稍小于失败几率(比值为 $(36^{24}-35^{24}):35^{24}\approx0.4914:0.5086$)。德·梅莱知道答案后惊讶不已。

在德·梅莱等一些赌徒朋友的影响下,帕斯卡开始思考"骰子博弈"中更一般的数学问题。而那些赌徒们虽然都精明过人,却无法理解他的思想。帕斯卡于是写信向父辈的朋友费马"请教"("挑战"?)。他们主要讨论了以下两类"赌金分配"问题。

掷点赌金分配问题 赌徒甲和乙约定:甲掷骰子8次,只要出现一次6点就可拿走全部赌金。后因故双方同意,甲停止进

行第 1 到第 4 次的投掷。那么根据公平合理的原则，甲每次停止投掷各应分得多少赌金？（费马的解答是：甲第 1 次停止应得到全部赌金的 1/6，因为他原来有 1/6 的获胜机会；同理，第 2 次停止应得到剩下赌金的 1/6，即全部的5/36；第 3 和第 4 次停止则分别应得全部赌金的25/216和125/1 296。）

掷胜赌金分配问题　赌徒甲和乙各拿出 32 元钱作为赌金，并约定每盘以掷骰子定胜负，谁先胜 3 盘就赢得全部赌金。现在假设甲以 3 比 0 赢得全部赌金，问其每一盘胜利的赢钱价值各为多少？

帕斯卡的解答是：第 1 盘和第 2 盘各赢了对手 12 元，第 3 盘赢了 8 元。其分析如下：当甲以 2 比 1 的局面领先时，下回合投掷如赢了则以 3 比 1 获得全部 64 元赌金；如输了则以 2 比 2 打平，双方以后的获胜机会相等；因此可以合理地认为，局面 3 比 1 的价值为 64 元，局面 2 比 2 的价值为 32 元（保本赌金），从而局面 2 比 1 的价值应为 48 元。当甲以 2 比 0 的局面领先时，下回合投掷如赢了则以 3 比 0 获得全部 64 元赌金；如输了则形成 2 比 1 的局面，已知道其价值 48 元；于是局面 2 比 0 的价值应为 56 元。当甲以 1 比 0 领先时，下回合如赢则形成 2 比 0 的局面，其价值 56 元；如输则成为 1 比 1，其价值显然是 32 元；所以局面 1 比 0 的价值应为 44 元。因此，3 比 0，2 比 0，1 比 0 和 0 比 0 局面的价值分别为 64 元，56 元，44 元和 32 元。依次相减就得到了帕斯卡的答案。

从现代概率理论来看，帕斯卡和费马所讨论的问题属于求

解离散概率的“**数学期望**①”和“**条件数学期望**”。并且，他们在解题过程中或澄清或隐含了一些关键概念。例如，每一次掷骰子都是一个独立的随机事件，其发生的概率不受之前结果的任何影响；离散随机事件的发生概率等于发生该随机事件的组合数与所有可能的组合数之比，等等。特别是，帕斯卡还分析了更一般的“赌金分配”问题，如在“掷胜赌金分配”问题中，规定“先胜 8 盘(或任意盘)者赢得全部奖金”，则此时首盘胜利的价值多少？又假设有 3 人甚至更多人参加此类赌局，则情况如何？

由于以上的成果，所以人们认为帕斯卡和费马开创了近代概率理论。其中帕斯卡作出了主要贡献。

帕斯卡为解答以上那些问题，不得不需要大量计算各种组合数；在没有计算机的时代，这是一项艰难的工作。为了提高效率，帕斯卡发明了计算组合数用的数字三角形，并专门写了《算术三角论》一书，介绍其用法。西方社会因此称之为“帕斯卡三角”。该三角形的结构特征是两边都是数字 1，从上到下依次形成各数字层，其中第 $n+1$ 层中的数字其实是二项式 $(1+x)^n$ 的展开式中 x 各项乘幂的系数；还有，下层中的每个数字正好是其上层相邻两数字之和(图 3-5)。

其实，在此 600 年前，中国北宋时期的贾宪(活动于约 1050 年)已经知道这种三角形。200 年后，南宋人杨辉(约 1261—1276 年)在其著作《详解九章算法》中做了介绍。因此在中国被称为“贾宪三角”或“杨辉三角”(图 3-6)。中国古代数学家用此

---

① 某一随机事件的“数学期望”被定义为发生该事件的概率与发生该事件后所得收益的乘积。

三角形计算高次方程的根。

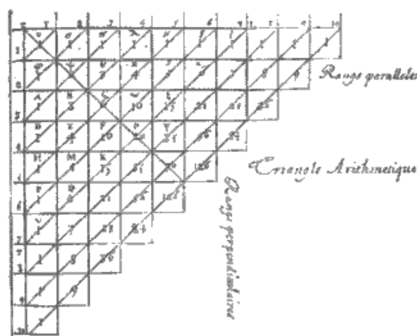


图 3-5 《算术三角论》一书中的帕斯卡三角



图 3-6 杨辉《详解九章算法》中的贾宪三角

帕斯卡虽然活了不到 40 岁，却取得了广泛的科学成就：除了概率论外，他在几何学与分析学中也有重要的开创性工作，对于牛顿和莱布尼茨有直接影响；在物理学领域，他发现了气体和液体压力的变化规律——现在使用的标准压强单位“帕斯卡”，就是为了纪念他的贡献；他还制造了第一台机械式计算机，被认为是现代计算机的鼻祖。他同时是一位极有影响的西方近代哲学家。在其传世名著《思想录》中，帕斯卡提议运用他所创立的概率论方法来处理信仰问题：

> 上帝可能存在也可能不存在。当你选择信仰上帝时，如上帝确实存在，则你将赢得永恒的生命和幸福；如上帝不存在，则你的损失也有限。比较永恒的所得和有限的所失，所以你应该选择信仰上帝。

一个令人深思的问题是，中国的麻将为什么没有产生概率

论？麻将可以当作游戏，也可以成为赌博。参与者明显地觉察其中有随机现象，感受到某些事件的发生有概率大小的问题。但是，这里面没有数学期望，没有事件独立性的思考，更没有大数定律的支撑。一切都停留在感觉上，也就没有科学可言。

3. 1933 年的革命性进展

公理化概率论的建立 帕斯卡和费马以后的近三百年，属于古典概率论的发展时期。古典概率论主要研究离散型随机事件，如掷骰子、抛硬币、发牌、摸彩，等等；其研究方法通常采用组合理论。但是，现实中有大量的连续型随机事件例子。比如说，人的身高和体重的分布，分子运动速度，设备零件的寿命，等等。此类问题是不能用组合方法解决的。另外，人们那时还没有完全搞清，“概率”究竟为何物。也就是说，概率论的理论基础并不健全。因此，它还不是一门成熟的学科，其应用也有限。

直到 1933 年，苏联数学家柯尔莫哥洛夫（Андре́й Никола́евич Колмого́ров，1903—1987）发表了一本 30 多页的小册子，题名叫《概率论基础》：其中运用公理化方法给出了概率论的严格定义；并引进法国数学家勒贝格（Henri Léon Lebesgue，1875—1941）不久前创立的测度论作为强有力的工具，从而能够统一处理包括离散型和连续型在内所有形式的随机变量。由于柯尔莫哥洛夫的这一开创性工作，使得概率论成为一门带有纯粹数学色彩的应用数学，进而为概率论的理论研究和实际应用开辟了广阔的天地。

数学小知识 柯尔莫哥洛夫的公理化概率论的框架大致

如下。

对于任何一个给定的随机现象的研究课题，定义一个“概率空间”，它由样本空间 Ω，事件域 F 和概率 P 组成，记为 (Ω,F,P)。其中：

(1)样本空间 Ω 是由全体基本事件组成的集合。如掷一粒骰子的样本空间是 $\{1,2,3,4,5,6\}$，掷两粒骰子的样本空间是 $\{(1,1),(1,2),\cdots,(6,6)\}$，人体身高的样本空间可以定义为 $(0,\infty)$，分子运动速度的样本空间可设为三维欧氏空间，等等。

(2)事件域 F 是一个以 Ω 的若干子集为元素的集合，它满足以下三条公理。

(i)$\Omega\in F$；

(ii)$A\in F\Rightarrow\overline{A}\in F$；

(iii)$A_n\in F(n=1,2,\cdots)\Rightarrow\bigcup\limits_{n=1}^{\infty}A_n\in F$；

其中 Ω 称为“必然事件”，$\overline{\Omega}$ 称为“不可能事件”。

(3)概率 P 是定义在事件域 F 上的一个集合函数，它满足以下三条公理。

(i)对于所有的 $A\in F$，有 $P(A)\geqslant 0$；

(ii)$P(\Omega)=1$；

(iii)P 具有**可列可加性**。

然后定义了“随机变量”，它们是从样本空间 Ω 到直线的一些映射，并定义了关于任意随机变量的“概率分布函数”，这些概念都与**勒贝格可测集**和**勒贝格积分**有关。利用这些概念，能够以标准方式解决包括求各种数学期望在内的一大类概率理论和应用问题。


图 3-7 柯尔莫哥洛夫

柯尔莫哥洛夫的母亲在生他时难产去世。他的父亲一直被流放，直到十月革命后回来任苏维埃农业部官员，不久战死沙场。他由姨妈抚养长大。成年后柯尔莫哥洛夫曾做过列车员，在业余时间坚持学习。1920 年进入莫斯科国立大学，开始时学习冶金和历史。有一次，他写了一篇关于 15—16 世纪俄国历史的论文。他的老师批评说："你在论文中只提供了一个论据。如果研究数学，那么一个论据已足够；但是我们研究历史的至少需要 10 个证据。"因为不想花费太多的时间寻找多余的证据，他于是改学数学。

除了奠定现代概率论基础之外，柯尔莫哥洛夫在众多的数学领域作出了重要贡献，他是 20 世纪最杰出的数学家之一。1980 年，他因在傅里叶分析、概率论、遍历理论和动力系统中深刻和开创性的工作而获得了沃尔夫数学奖；1986 年获得国际罗巴切夫斯基几何奖；他同时是多个国家的科学院院士。

未来之舟

在柯尔莫哥洛夫之后，概率论迅速发展成为一门兼具纯粹数学和应用数学特点的数学分支，并且得到广泛的应用。它不仅为数理统计、随机过程、动力系统、控制论、信息论、生物数学、数值计算等一大类应用数学，以及物理学、计算机科学、经济学等多门学科提供了必要的理论基础，而且在人类三大产业的生产活动以及文化生活等各方面，发挥了至关重要的作用，如证券业、保险业、企业质量管理、体育竞技、科学实验活动等，现在都已离不开概率论所提供的概念和方法。

3.2　第二次世界大战中的数学密码学

第二次世界大战的胜利，包含着许多数学家的努力。运筹学诞生在战场，火炮自动控制导向数学控制论；流体力学理论服务于 B-52 轰炸机的设计；更不要说计算机的研制标志着信息时代的来临。这里要说的是另一个没有硝烟的战场：密码破译。

1. 古代的密码

保密通信在战争中应用的历史源远流长。它可以追溯到2500年前，古希腊的奴隶主，在剃光了头发的奴隶头上写字，然后等头发长出来，再令他到另一处去传递情报。当时的希腊军队里，还使用一种叫做 scytale 的通信方法（图 3-8）：把长带子状羊皮纸缠绕在一根圆木棍上，然后在上面写字；解下羊皮纸后，上面只有杂乱无章的字符，只有再次以同样的方式缠绕到同样粗细的棍子上，才能看出所写的内容。2000 年前，古罗马的执政官和军队统帅凯撒（Julius Caesar，公元前 100—公元前 40）发明了一种把所有的字母按字母表顺序循环移位的文字加密方法（图 3-9）。

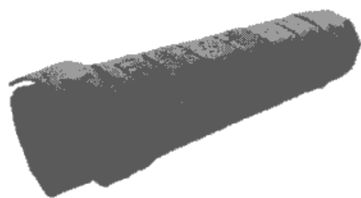


图 3-8　古希腊人用于保密通信的 scytale



图 3-9　用于产生凯撒密码的字母循环移位盘

总的来说，密码术在古代的保密通信技术中并不占很重要的地位，也没有对任何战争的胜负产生决定性影响。因为那时异地通信的主要方式是采用文字书信，只要能够防止有关书信落入敌人手中，文字不加密也不会有大问题。

然而，自从1844年发明了电报和1901年发明了无线电通信以后，情况开始发生了根本性的变化。由于无线电报能够快速方便地进行远距离收发，它很快成为战争中主要的通信手段。但无线电报是一种广播式通信，任何人，当然包括敌人，都能够接收到发射在天空中的电报信号。于是，为了防止机密泄漏，密码术开始变得至关重要。

在第一次世界大战中，德、英、法等国都设立了密码局，交战双方的密码专家们开始斗法。争斗中，大家互有胜负：德军截获到俄军的无线电通信，洞悉了其军事部署，结果把拥有优势兵力的俄国人打得大败，战败的俄国不久在国内爆发了十月革命；法国人则数次破译了德军的密码，成功地粉碎了德军攻占巴黎的行动。这场争斗的最后输家还是德国：俄军在德国的一艘巡洋舰上缴获了一本德国海军用的密码手册，并把它交给了盟友英国人，结果德军大量的密码被破译，遭受到严重损失。

1917年，英国人破译了德国外交部长齐默尔曼发给德国驻墨西哥大使并要求转交给墨西哥总统的一份绝密电报，电报中告知，德国将重新开始“无限制海战”，用潜艇攻击包括美国等中立国在内的海上商运船，并建议墨西哥入侵美国，以阻止美国介入欧洲的战争，并承诺帮助墨西哥从美国手中夺回得克萨斯、新墨西哥和亚利桑那三州。英国人把电报的内容透露给了美国

人，美国人因此勃然大怒，于是向德国宣战。第二年，德国被打败，宣布投降，接着签署了《凡尔赛条约》，大战结束。这是第一次世界大战中最成功的一次密码破译。

虽然密码的应用已经在第一次世界大战中大显身手，但密码学作为一门学科，在当时并没有很大的发展。使用的加密方法与古代相比并没有什么创新，只是增加了一些难度。

2. 现代的"隐谜"密码机

德国电气工程师谢尔比乌斯（Arthur Scherbius，1878—1929）在 1918 年发明的"隐谜"密码机，带来了密码技术的一场革命。

"隐谜"是世界上第一台电气机械装置的密码机，其形状如同一台打印机（图 3-10、图 3-11）。

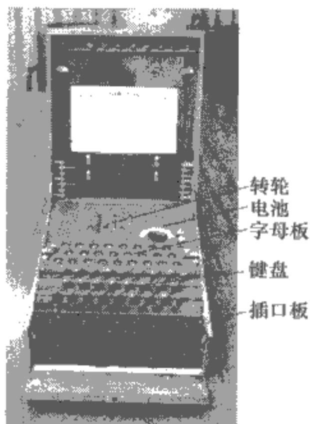


图 3-10　"隐谜"密码机



图 3-11　转轮及其解剖图

从图 3-10，图 3-11 中可以看到，"隐谜"密码机由键盘、字母板、转轮、反射轮（固定在密码机内，其结构同转轮）和插口板组

成。其加密过程如下：

(1)设好 3 个转轮的初始值，并用 6 根插头电线连好插口板上的 6 对插口；

(2)在键盘上打明文，每打一个字母，该字母信号就会通过相应的电线传到插口板；

(3)在插口板上，如果该字母正好属于 6 对连接起来的插口中的一对，则互换字母，否则不作互换，通过接线圆环把字母信号传到右面第一转轮上；

(4)该转轮通过内部电线的连接方式，对输入的字母作替换，然后传到中间一个转轮；同时自己转动一格；

(5)中间的转轮再对字母作替换，然后传到左边一个转轮；这时如右边转轮正好从 25 格转到 0 格，则自己也转动一格，否则不转；

(6)左边的转轮再对字母作替换，然后传给最左边的反射轮；这时如果中间的转轮正好从 25 格转到 0 格，则自己也转动一格，否则不转；

(7)反射轮也对字母作替换，然后传回给左边转轮；反射轮永远不转动；

(8)字母信号再从左边转轮、中间转轮、右边转轮和插口板依次传回，每经过一处都要作一次字母替换；

(9)最后，信号传到字母板上，使相应字母下面的小灯泡闪亮，这就是加密后的字母。

由于反射轮的作用，使得“隐谜”的解密变得很简单，其过程与加密相同。在设定好了与加密时一样的转轮初始值和插口接

线后，在键盘上打入密文，则经过以上步骤后，在字母板上就显出了明文。

从以上的加密过程可以看到：从明文到密文，一个字母要经过至少 7 次至多 9 次的替换，而且对于转轮的不同状态、插口板的不同连接以及套接圆环上不同的字母排列顺序，其替换都是不同的；所以"隐谜"的加密方法要比以往任何的加密方法复杂得多。谢尔比乌斯因而在向德国海军推销自己的产品时，很自信地说，即使敌人拿到了一台"隐谜"机，也破解不了密码；即使他们掌握了"隐谜"机的加密原理并获得了一部分密码，也发现不了密钥（即"隐谜"机的初始设定）。

开始，"隐谜"机的市场销售并不好。后来，德国人意外地从丘吉尔的回忆录中得知，在第一次世界大战中，自己的密码系统早被英国人破译，因此遭受了惨重损失。德军于是开始着手改进自己的密码系统。这时，他们看中了"隐谜"机这一革命性的密码装置。1926 年，海军开始采购"隐谜"机，同时要求对它进行彻底的改装，使得它比商用的"隐谜"机更复杂更安全；两年后，德国陆军也开始使用。1933 年，纳粹上台。不久，希特勒撕毁《凡尔赛条约》，开始肆无忌惮地扩充军备，"隐谜"机则成为德军最重要的秘密通信工具。

3. 波兰数学家首作贡献

第一次世界大战后的波兰，处于一种尴尬的境地。她东邻苏联，西接德国；两个强大的邻国一直在虎视眈眈，觊觎着她的领土。当时的波兰就像一只身处险境的野兔，要时刻竖起警惕

的长耳，留心着不怀好意的邻国的一举一动。隶属于波军总参谋部情报机构的密码局，就是波兰的长耳，它一直在监听国外的无线电通信。

虽然波兰的国力远不如她的邻国，却拥有欧洲顶尖的密码技术。他们对德国人的密码系统一直了如指掌。然而，到了1928年，波军密码局发现德军开始使用一种全新的密码，这种新密码根本无法破解，这使他们日益感到不安。

不久，他们做出了一个很有远见的决定：培养数学专业的学生来帮助破译德国人的密码。当时的这种做法实属一项创新举动，因为那时人们都认为破译密码不需要多少数学知识，许多国家都请语言分析专家、纵横字谜高手和国际象棋冠军来破译密码，很少找专业的数学家帮忙。后来的事实证明，只有采用数学方法，才能对付“隐谜”这样的密码。

1929年1月，波兰波兹南大学数学系的一群20多岁的大学生和部分研究生被要求宣誓保密，然后开始学习一门密码学课程。学生们每周上两个晚上的课，几个星期后就开始破解各种密码，那些无法完成破解功课的学生则被淘汰。随着课程的深入，破解的密码越来越难，过关的学生也越来越少。最后只剩下3名最优秀者，他们是雷耶夫斯基(Marian Rejewski，1905—1980)、齐加尔斯基(Henryk Zygalski，1907—1978)和鲁日茨基(Jerzy Różycki，1909—1942)。正是这三位年轻的波兰数学家，后来破译了曾经被认为是不可能被破译的“隐谜”密码。其中雷耶夫斯基居功至伟。

1932年夏，雷耶夫斯基、齐加尔斯基和鲁日茨基，三人一起

正式加入了密码局。同年10月，密码局的头头就把那个谁也拿它没办法的德军新密码交给雷耶夫斯基破译。令他们喜出望外的是，这位年轻人在数周之内就取得了进展。



图3-12 雷耶夫斯基 图3-13 齐加尔斯基 图3-14 鲁日茨基

由于常规的破译方法对于“隐谜”密码毫无作用，雷耶夫斯基决定另辟蹊径，从分析密码机的工作原理着手。他发现从数学的角度来看，密码机的作用就是对26个字母进行置换，而所有可能的置换通过合成关系形成了一个置换群。

数学小知识 所有的n个元素的置换通过合成关系形成了一种代数结构，叫做“置换群”。置换群首先由19世纪法国天才数学家伽罗瓦(Évariste Galois，1811—1832)发现，他通过研究多项式方程根的置换群结构，获得了方程有无根式解的判定条件。

雷耶夫斯基于是建立了“隐谜”的置换群方程，并断定只要解出这些方程，就能够破解它的密码。但是在一般情况下置换群的结构很复杂，所以这些方程几乎无法解出。幸运的是，他发现了“隐谜”两个致命的弱点，使得局面完全改观。

其中一个弱点来自于密码机的结构。如上一小节所述，密

码机上有个反射轮，由于该轮的作用使得加密和解密的过程完全一样，即如果键入字母 a 得到 x，则键入 x 就得到 a。如此操作当然很方便，但对于密码的安全来说，这种方便是一场灾难。雷耶夫斯基发现，由于“隐谜”的这一功能，使得它的置换群结构变得简单：所有的置换都是字母的两两对换。这就大大降低了求解置换群方程的难度。

“隐谜”的第二个弱点来自于它的操作规程。如前所述，每份“隐谜”电文的开头都有一组 6 字母的密钥字符串，它是通过把反映转轮初始位置的 3 字母密钥重复加密得到的。重复加密的目的是为了确保接收方能够获得解密电文所需的密钥，但它也提供了雷耶夫斯基求解置换群方程的钥匙：比如说，在某天“隐谜”的某一份密文中，其起首的密钥字符串为 $d\quad m\quad p\quad v\quad b\quad m$，则可以假设加密前相应的明文字母是 $x\quad y\quad z\quad x\quad y\quad z$，这 $x\quad y\quad z$ 三个字母就是该电文的密钥，也就是加密电文时 3 个转轮的初始位置参数，它们对于破译者来说是未知的。用置换的语言来描述：如果假设密钥字符串上第 1 个位置上的置换为 T_1，第 2 个位置为 T_2，…，第 6 个位置为 T_6。则有

$$T_1(x)=d,T_2(y)=m,T_3(z)=p,$$

$$T_4(x)=v,T_5(y)=b,T_6(z)=m。\qquad(1)$$

其中 $T_1,\cdots,T_6$ 当然是未知的。但是根据以上分析，知道 $T_1,\cdots,T_6$ 都是两两对换的置换。所以有 $T_1(d)=x,T_2(m)=y$，$T_3(p)=z$。于是从式(1)可以得到

$$T_4(T_1(d))=v,T_5(T_2(m))=b,T_6(T_3(p))=m。\qquad(2)$$

这样，如果令置换 A 为 T_1 和 T_4 的合成，B 为 T_2 和 T_5 的合成，

C 为 T_3 和 T_6 的合成，则置换 A,B,C 是部分可知的。雷耶夫斯基观察到，只要一天能够截获 80 份“隐谜”密文，则 26 个字母都会在密钥字符串的 1 到 6 的每个位置上出现。这样就可以完全决定置换 A,B,C！雷耶夫斯基把这三个置换称为这一天“隐谜”密码的“特征集”，因为它在一天里不变。

下一步是要通过特征集求出 $T_1,\cdots,T_6$。注意到 $T_1,\cdots,T_6$ 都是两两对换，所以特征集中的置换都是由两个两两对换合成的，雷耶夫斯基证明了这样一条关于两两对换合成的置换群定理。

定理　在由两个两两对换合成的置换中，所包含的长度相同并且不相交的圈的个数总是为偶数；反过来，如果一个置换中出现的长度相同并且不相交的圈的个数总是偶数，那么，它一定可以分解为两个两两对换的合成。（说明：如果在一个置换中，把两两不同的元素 a_1 换成 a_2，a_2 换成 a_3，…，a_n 换成 a_1，则称该置换包含一个长度为 n 的圈，记为 $(a_1a_2\cdots a_n)$。例如，“两两对换”其实就是长度为 2 的圈。）

这条定理被人称为是“打赢第二次世界大战的数学定理”！它给出了求解 $T_1,\cdots,T_6$ 的方法：只要找出特征集置换的所有对换合成就可以了。

再下一步是要确定转轮上的接线方式。从理论上讲，只要通过比较多天的特征集并利用置换群方程(2)，就能够做到这一点。当然，这需要很复杂的计算。然而，雷耶夫斯基的面前突然出现了一条捷径。

1932 年 12 月，法国密码局局长贝特朗造访波兰密码局。他

随身带来一包东西，里面是德军关于“隐谜”密码机的操作手册和1932年9月和10月两个月里每天“隐谜”的初始条件值，即转轮的排列与起始位置以及插口板上的接线方式！原来这些材料是德国密码局中负责掌管“隐谜”资料的军官施密特为了赚钱而出卖给法国人的。但是法国人拿到这些东西却不知道如何利用。因为法国和波兰有情报合作协议，所以就复制了一份送给波兰密码局。

雷耶夫斯基拿到了这些宝贵的材料后，立即利用其中详细的数据算出了每个转轮上的接线方式。至此，德军使用的“隐谜”密码机的结构已经完全清楚了。为了进一步破译的需要，波兰密码局立即仿制了数台“隐谜”机。这是在1932年年底，就在这个时候，雷耶夫斯基的两位同学，齐加尔斯基和鲁日茨基，也加入了破译“隐谜”的队伍。

这三位年轻的波兰数学家先后设计了回转机、穿孔纸和“炸弹”机等设备。其中回转机相当于把两台“隐谜”机对接，而“炸弹”机(据说这一名字是鲁日茨基借用当时的一种冰淇淋名而得来的)相当于把六台“隐谜”机连接在一起。有了这些设备，就能针对德军“隐谜”机不同的使用情况，获取其每天的初始设置参数。至此，“隐谜”遂告破解。以后几年，波兰密码局每天都破译大量的德军电报。

如果说谢尔比乌斯发明的“隐谜”机标志着机器加密时代的开始，那么波兰年轻数学家设计的“炸弹”机等设备则宣告了机器破译日子的来临。

随着德国法西斯越来越咄咄逼人，战争已渐渐临近。德军

对“隐谜”的改进越来越频繁。他们先后更换了反射轮，把插口板上的6对接线增加到10对，并且把3个固定的转轮增加到了5个，然后每天从中任选3个使用。

新的改进措施给波兰人的破译工作带来了一时难以克服的困难。而战争已经迫在眉睫。这时，波兰密码局审时度势，做出了一个重要的决定。

1939年7月24—26日，英国、法国和波兰的密码局官员们集中在波兰密码局开会。三位波兰年轻数学家出席了会议。会议期间，英法的代表们各自收到波兰同行们送的一份意外的礼物：复制的德国军用“隐谜”密码机、“炸弹”机、穿孔纸，以及关于破解“隐谜”密码数学理论和技术方法的详细说明等等。面对这份礼物，英国人和法国人都目瞪口呆：原来他们的波兰同行早已破译了“隐谜”！而他们自己长期以来一直想方设法破解它，却没有取得任何进展。

一个多月之后，1939年9月1日，德国大举入侵波兰，勇敢的波兰骑兵与德国坦克部队进行了一场力量悬殊的战斗。两个星期之后，苏联开始进攻波兰。数天之内，波兰就被两个大国解体瓜分。英法两国则向德国宣战。第二次世界大战爆发了。

4. 英国的布雷契莱庄园

虽然波兰人天才地破译了早期的“隐谜”密码，但以他们的数学能力和国家实力尚不能或来不及应付德国人后来对“隐谜”的一系列改进措施，最终无法阻止亡国之灾。所幸的是，他们及时地把破译的关键技术和设备传交给了英法两国。然而，波兰

沦陷后不到1年，法国人还来不及改进波兰人的成果，就被德国的闪电战一举击败，只得宣布投降。于是，继续破解“隐谜”以争取反德国法西斯战争胜利的重任，很自然地落到了英国人的肩上。

距英国首都伦敦西北约75公里，有一座20世纪60年代才设立的新兴城市，叫做米尔顿凯因斯(Milton Keynes)市，位于该市的西南部有一个小镇，叫做布雷契莱(Bletchley)镇，镇上有一个占地22公顷的庄园，叫做布雷契莱庄园，该庄园是第二次世界大战中英国最神秘的地方。因为英国于1939年将其负责截听和破译国外无线通信的情报机构秘密地搬入此地，该机构的公开名称叫做“政府密码学校”。德国人做梦也没有想到，这个破旧的庄园中隐藏着英国人最致命的战争武器，其作用甚至超过一千架飞机、一万辆坦克和一百万精锐部队。在整个第二次世界大战期间，缺乏防卫设施的布雷契莱庄园几乎没有遭受过敌机的轰炸。



图 3-15　布雷契莱庄园

布雷契莱庄园的“政府密码学校”在鼎盛时期拥有约9 000名工作人员。其中有不少国际象棋冠军、纵横字谜高手和通晓多国语言的专家，这几类人一直是传统密码战场上的主力军。“学校”有时会采用一些别出心裁的方法来招募人才。如有一次，他们请《每日电讯报》举办一场纵横字谜比赛，凡是在12分钟内完成字谜游戏的参赛选手都被询问“是否愿意从事一种能为战争作贡献的特殊工作”。

波兰人的成功终于让英国人认识到，要破解像“隐谜”这样的现代密码，数学家才是最合适的人选。“政府密码学校”马上从英国著名学府剑桥大学召来三位优秀数学家，他们是杰弗里斯、威尔仕曼和图灵，连同前些时候进来的特温，这4位数学家分别为破解“隐谜”作出了不同的贡献。

然而，毫无疑问，对破解“隐谜”机作出最大贡献的是阿兰·图灵(Alan Mathison Turing，1912—1954)——20世纪杰出的数学家、现代计算机科学的奠基人。

来到布雷契莱庄园之后，图灵开始重新思考有关“隐谜”破译的问题。他发现波兰同行的破译方法依赖于对每份“隐谜”电文前被重复加密的3字母密钥的分析，这种做法有很大的局限性：一旦德国人对机器结构和操作规则稍加变动，就会导致方法失灵，只能推倒重来。事实上，当时波兰人的方法已经很难奏效。因此，必须尽快找到新方法。

前面已经指出，雷耶夫斯基发现了“隐谜”机的一个严重缺陷：它的加密置换群总是由字母的两两对换构成，即如果把A加密成Q，则一定会把Q加密成A，利用这个缺陷，雷耶夫斯基解出



图 3-16　图灵和他在布雷契莱庄园的工作场所：八号棚屋

了加密过程的置换群方程。图灵经过仔细分析“隐谜”机的工作原理，发现了它的又一个严重缺陷，那就是它永远不会把一个字母加密成本身，即永远不会把 A 加密成 A，把 B 加密成 B，等等。利用这一缺陷，图灵提出了一种基于 crib 的破解方法。

“crib”的原意是指考试作弊时的夹带，在这里表示一段未加密的文字或字符串。图灵的新破解方法如果用手工来操作，则大致如此：设已确认一份加密电文中包含了一段 crib 内容，则将密文与 crib 上下并排对齐，然后逐个位置比较上下字母；如至少有一个位置的上下字母相同，则将 crib 右移一位，继续比较；直到发现两者在所有的对应位置上没有相同的字母，则密文中的这段字符串很可能是对应 crib 内容的加密文字，于是得到这些位置上的一些加解密字母之间的对应关系。可以证明，只有少量的“隐谜”机转轮的组合设置才能够正好在那些位置上将给定的 crib 加密成所对应的字符串，从而排除了大量的不符合要求的转轮组合设置，使得进一步的破译工作大大简化。据统计，一份加密电文中只要含有 30 个字母左右的 crib 就可以被破解。

图灵方法需要利用足够多的 crib。那么，如何找到它们？

事实上，利用德国人刻板的行文风格和密码机操作上的漏洞，不难找到所需的 crib。如某台“隐谜”机总要准时发送该地区的天气预报，这段电文总是以“VORHERSAGEBEREICH SIEBEN”(七号地区的天气预报)开头，这给英国人提供了所需要的 crib。

有时，由于种种原因，德国人会把同样的电文内容用新旧两种参数加密各发送一遍；这时就有可能利用旧参数加密发送的电文作为 crib 来破解新参数的密文了。这种 crib 在布雷契莱庄园被叫做“接吻”。

还有些时候，为了获得所需要的 crib，英国人会刻意制造一些事件，引发德军在来往电文中使用某些词。如有意在某一地区布雷，当地的德军就会立即向上级报告，请求派工兵来扫雷。这样，在来往电文中一定会包含“地雷”这个词。这种获取 crib 的方法在布雷契莱庄园被称为“种花”，它屡试不爽。

如果真的用人工来实现图灵的方法，则需要花费大量的时间，效率太低。因此，必须使用机械和电气化的手段。图灵于是和威尔仕曼以及英国制表机公司的总工程师基恩(Harold Keen，1894—1973)合作，改进了波兰人发明的“炸弹”机。改进后的装置仍然叫做“炸弹”，只是其名称的字母拼写从波兰人的“Bomba”改成英国人的“Bombe”。英国人所以仍然使用这个名字，是因为这种机器运转的时候会发出钟表一样的嘀嗒声，就好像一颗上了发条的定时炸弹。“炸弹”机上有 36 组转轮，每组中有 3 个转轮，所以它实际上相当于 36 台“隐谜”机的组合。而雷耶夫斯基原先设计的旧“炸弹”机相当于 6 台“隐谜”机的组合。在第二次世界大战期间，英国人共造了 211 台“炸弹”机，破译了

德军90%以上的“隐谜”电文,为赢得战争的胜利作出了重要的贡献。

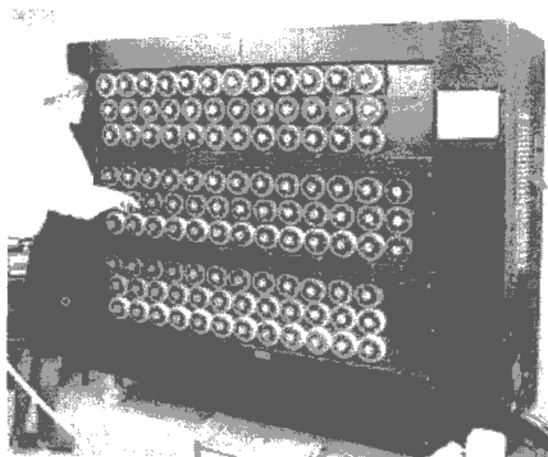


图3-17 专门破译“隐谜”密码的英国“炸弹”机

图灵还负责破译德国海军的“隐谜”密码。这在布雷契莱庄园被认为是最困难的任务。德国海军历来极其重视无线通信的可靠性和保密性,它率先在德军中使用“隐谜”密码机。在第二次世界大战中,德国海军的U-潜艇舰队平时悄无声息地潜行在大西洋海中,直到发现合适的目标——美英运输船队——后,才通过无线电报召来同伙以“狼群”战术展开凶猛的攻击。无线保密通信对于潜艇舰队的生存和胜利至关重要。因此,德国海军即使对于所信赖的“隐谜”机也频繁地加以结构和操作方式改进,以确保它无懈可击,绝对可靠。

第二次世界大战前夕,德国空军和陆军的“隐谜”机的转轮从3个增加到5个(每天按规定选用其中3个)。这已经给波兰破译者带来了巨大的困难。而德国海军“隐谜”机的转轮又继续增加到7个,最后增加到8个(每天按规定选用3或4个)!

在图灵来到之前，布雷契莱庄园中几乎所有人都认为德国海军的“隐谜”密码是无法破译的，因此没有人愿意为它浪费时间。图灵来了之后，虽然不久发明了基于 crib 破解方法的“炸弹”机，但由于德国海军的“隐谜”机有 8 个备用转轮，比德国空军和陆军的“隐谜”机多用 3 个，使得前者可能使用的密码变化范围要比后者大得多；而早期的“炸弹”机运行不太快，所以它们破解德国海军密码的效率很低。

鉴于德国的 U-潜艇正在严重威胁盟军的大西洋生命线，寻找有效的破解德国海军“隐谜”密码方法已成为刻不容缓的任务。图灵经过一段时间的摸索和研究，终于发明了基于贝叶斯(Thomas Bayes，1702—1761)统计原理的“班布里方法”，之所以取这个名称是因为实行此方法所用的卡片是在英格兰中部一个叫做“班布里”的地方制作的。

班布里方法基于语言学中这样一个统计事实：把任意的两段文字拿来排成行，上下对齐作比较，查看其中有多少对字母是相同的。则当这两段文字属于同一编码系统时出现相同字母对的概率明显高于当它们不属于同一编码系统时的相应概率。特别地，对于德文来说，如果两段文字是用不同的方法加密的，则相当于字母的随机配对，其出现相同字母对的概率为 1/26；而如果两段文字都是没有加密的明文或是按相同方式加密的密文，则出现相同字母对的概率为 1/17。

1940 年 5 月 8 日，用班布里方法破解德国海军的“隐谜”密码首次获得成功。以后三年里，此方法结合“炸弹”机成为英国人破解德国海军密码的主要手段，为盟军重创德国潜艇舰队，守

住大西洋生命线作出重要贡献。一直到 1943 年 9 月，此时“炸弹”机的性能已经有大幅度的提高，只需数十分钟就能破译一份“隐谜”密码，班布里方法才被停止使用。

未来之舟

由于雷耶夫斯基和图灵等人在密码战线上的卓越工作，使得盟军能够屡创法西斯军队，并最终赢得了第二次世界大战的胜利。这几位杰出数学家还开创了数学在密码学中的应用，并成功实现了利用机械设备破译密码。第二次世界大战以后，由于网络通信的普及，使得密码学迅速发展。而数学在其中起了决定性的作用，以至今天的密码学实际上已成为数学的一个应用分支。另外，计算机也已被广泛用于密码的加密解密中。本章下一节将进一步介绍现代密码学的发展。

3.3 开创数字时代

——仙农与他的信息论

21 世纪是信息时代，也被称为数字时代，因为这一时代的基本特征就是信息的数字化。各种信息被转化成一串串二进制数，它们储存在光电磁介质中，然后由功能强大的计算机处理，并通过四通八达的通信网络传送，结果使我们的世界发生了奇妙的变化。

大量语言、文字、图像、声音和影视信息已被数字化：人们开始用计算机写文章，坐在家中方便地通过网络查找并浏览所需要的各种文献、资料和信息，下载或在线欣赏无数的音乐、歌曲、电影和电视节目。

数字化信息提供了新的丰富多彩的人际交流方式：电子邮件、网上聊天、博客等等，人类从来没有能够像今天这样，可以跨

越时空界限，无拘无束地同那么多认识或不认识的人开展交流，自由自在地在网络上展现自我。

数字化为我们提供了新奇的产品：数字电视、数码相机、移动电话、数码音乐、卡拉 OK，等等。

数字化信息还带来了学习、工作和生活方式的变化：人们已经可以实现远程教育、网上办公、远程诊断、电子商务、网上购物，等等。

数字化也带来了新的观念。大家开始谈论数字化图书馆、数字化城市、数字化地球、数字化经济、数字化生存……

数字时代已经给我们带来那么多梦幻般的变化，并且还在继续制造更多神奇。而所有这一切的起源，都要追溯到一位名叫仙农的美国人和他所创立的信息论。

1. 从"开关代数"起步

仙农（Claude Elwood Shannon，1916—2001）出生于美国密歇根州佩托斯基（Petoskey）镇。"佩托斯基"之名源于当地印第安土著语，意谓"曙光"。这个坐落在密歇根湖边上的美丽小镇，常被美国作家海明威当作一些小说故事的发生地。

仙农的父亲是商人，曾经做过一段时期的法官；母亲是中学语文教师，当了几年校长。仙农小时候喜欢机械和电子，制作过模型飞机和遥控小船，甚至做了一套能工作的收发报机。他学习成绩最好的科目是数学。读书空余时间，靠送电报和



图 3-18　年轻的仙农

修收音机赚零花钱。

1932年从母亲的中学毕业后，仙农考进密歇根大学。4年后取得了电气工程和数学双学士学位。然后他来到著名的马萨诸塞理工学院（MIT），在电气工程系一边做助理研究员一边读研究生课程。1938年获电气工程硕士学位，其学位论文的题目是“继电器与开关电路的符号分析”。此文获得了美国工程师学会的“诺博奖”，当时有人称赞它“可能成为20世纪最重要和最出名的硕士论文”。

仙农在论文中首次证明了，“布尔代数”中关于“真值函数”[①]的“与”、“或”、“非”逻辑运算，与只有“0”和“1”两个数字符号的“二进制数”算术运算等价；而且可以用布尔代数中的“真”、“假”值或二进制数中的“0”、“1”数字，来表示继电器或电路的“开”、“关”状态；反过来，也可以用后者的开关状态来表示真值函数或二进制数。根据这一结果，他成功地运用布尔代数和二进制数运算的方法简化了继电器和开关电路系统的设计；同时指出，也可以反过来，用继电器和开关电路系统来解决布尔代数或二进制数运算问题。仙农的这些工作开创了一个叫做“数字电路”（也叫“逻辑电路”或“开关电路”）的新电子技术领域。该领域是将来设计各种自动控制系统和制造电子计算机的技术基础，也为后来信息论的创立埋下了伏笔。

1940年，仙农在MIT获得数学博士学位。学位论文题目是“理论遗传学代数”，其中试图建立一种描述生物染色体上基因

---

① 即只取“真”或“假”两值之一的函数（在逻辑学中称为“函项”）。

排列和遗传规律的代数方法。随后，他加入了著名的美国电话电报公司贝尔实验室。在二次世界大战期间，他主要为军方设计火炮控制系统和研究密码学。这两类工作均涉及数据或信息的传送、转换、破解、分析和利用，对于它们的研究帮助仙农形成了他的革命性思想。

2. 划时代的贡献

1948 年，仙农发表了那篇划时代的论文——"通信的数学理论"。该文的主题是要用数学方法确定通信线路的信息带宽和所传信号的信息量，以保证所设计的线路能够在排除噪声干扰的同时顺利地传送有关信号。为此，仙农给出了两个重要的定义：

信息的基本单位　信息的基本单位是二进制数的位，称为比特(bit)；如果一条通信线路能在 s 秒传送 N 位二进制数，则该线路的通信带宽就是 N/s(比特每秒)。

其中 bit 取自英文"二进制数位"的缩写。仙农指出，任何一个具有两种状态的事物——比如说继电器或开关电路——正好能够储存 1 比特信息。

信息熵的定义　假设在一个概率空间中包含有 n 件可能事件，它们的发生概率分别是 $p_1, p_2, \cdots, p_n$，则定义这些事件的熵为

$$H(p_1, p_2, \cdots, p_n) = -\sum_{i=1}^{n} p_i \log_2 p_i\ 。$$

信息熵是描述信源本身统计特性的一个物理量。它是信源的平均不确定度，是信源统计特性的一个客观表征量。不管是

否有接收者，它总是客观存在的。信息量则往往是针对接收者而言的，所谓接收者获得了信息，是指接收者收到消息后解除了对信源的平均不确定度，它具有相对性。因此，接收的信息量在无干扰时，在数值上就等于信源的信息熵。

这里，我们不妨联系具体情形做一些解释。中国古代的烽火台，它能传送两种情况：燃烽火或不燃（相当于 1，0）。在没有干扰的情形下，很自然地认为它能够传送一个比特的信息量。我们用以 2 为底的对数加以描写：$\log_2 2=1$。如果有两个烽火台，燃烽火分别表示“敌人来”和“要补给粮草”。那么总共可以表示四种情况：

(1)敌人来，要补给；

(2)敌人来，不要补给；

(3)敌人不来，要补给；

(4)敌人不来，不要补给。

于是，两个烽火台传送的四种情况，相当的信息量是：$\log_2 4=2$（比特）。

天才的仙农把信息量和概率联系起来，引入了信息熵的概念。事实上，上述的烽火台可传送的信息量，只在敌人可能来和不来的可能性差不多的情况下才有效。比如，当周幽王为博“褒姒一笑”，随便燃烽火，燃烽火的概率很大了，不稀奇了，传送的信息量也就小了。俗话说“狗咬人”不是新闻，“人咬狗”发生的概率小，才是新闻。仙农的论文里提到，“今天太阳升起”没有多少信息量，“今天日食”则有信息量。于是，仙农指出，事件发生的概率 $P(E)$ 大，则传送此事件后，接受者能够消除不确定性的

量(信息熵)$H(E)$就会小。这就有信息熵的定义,仍采用以 2 为底的对数,对各种可能事件发生的概率的对数,乘上相应的概率,加一负号,可以反映这是一个平均不确定性的度量。

例如,假定敌人来的概率是 1/2,那么不来的概率也是1/2,信息熵定义为

$$H(1/2,1/2) = -[(1/2)\log_2(1/2) + (1/2)\log_2(1/2)]$$
$$= -[-(1/2) + (-1/2)] = 1。$$

如果没有干扰,接受者获得的信息量就是信息熵,等于 1。

仙农指出,信息熵刻画了这些可能事件的不确定程度:当其中有一件是确定性事件(即发生概率为 1),则其他都是不可能事件(发生概率为 0),此时的熵值最小,等于 0;当这些事件发生的概率相等(即都为 $1/n$),则此时的熵值最大,等于 $\log_2 n$。所以在等概率可能事件的情况下,其不确定程度最大;并且可能的选择越多(即 n 越大),则不确定性越大。仙农进一步指出,信息熵与统计力学中的热学熵之间有联系。

仙农利用以上所给出的定义,成功地解决了有关线路带宽、信号传送和噪声干扰之间关系的一系列问题,由此奠定了现代通信理论基础。然而,他引进的这些概念所带来的影响远远不止于此。

数学小知识　我们在日常生活中通常使用十进制数;即用 0,1,2,3,4,5,6,7,8,9 这十个数字符号,按从右到左"逢十进一"的排位原则,来表示任意的整数。比如说,1 234 这个十进制数,实际上表示的数是 $4+3\times10+2\times10^2+1\times10^3$。人类所以采取十进制数可能与其在文明初期习惯用十个手指数数有关。

二进制数则只使用0,1这两个数字符号,按从右到左"逢二进一"的排位原则,来表示任意的整数。比如说

$$(11\,101)_2 = 1\times 2^0 + 0\times 2^1 + 1\times 2^2 + 1\times 2^3 + 1\times 2^4 = (29)_{10}$$

我们用括号加相应的下标来表明它是采用何种进制的数。

二进制数的优点之一是使用符号少,因此适合计算机处理和通信网络传输;优点之二是四则运算十分简单,比如说其乘法只有四条法则:0×0=0,0×1=0,1×0=0,1×1=1,(想一想小学生要花多少功夫才能背熟十进制乘法运算的九九表?)其缺点是数位太长,一个三位十进制数相等于一个十几位的二进制数。

从数学的角度来看,十进制数与二进制数是等价的。

3. 信息熵来源于热力学

热力学第二定律、麦克斯韦小妖与信息熵 19世纪德国物理学家克劳修斯(Rudolph Clausius,1822—1888)和英国物理学家开尔文(Lord Kelvin,1824—1907)所发现的热力学第二定律告诉我们:

一个封闭的热学系统总是随着时间的增长而趋向于一个温度处处相等的平衡状态。

或等价地说,

热不可能自发地从低温传到高温。

热力学第二定律解释了为什么宇宙时间不可逆转:比如说,茶杯里的水不会自行升温而沸腾;生命的历程不可能从老到幼

逆向进行;人类社会也不会倒退回去而使古人复活,等等。而按照牛顿的力学定律,时间在前进还是在倒退没有任何区别,因为任何一个力学过程都是可逆的。

热力学第二定律可以用数学语言准确地描述:

一个封闭的热学系统的熵总是随着时间的增长而增加,直到取得最大值,此时系统处于热平衡状态。

这里的"熵"是一个关于系统热量和温度分布的函数。

统计力学的理论和实验证实,气体的温度是由于气体内所包含大量分子的运动而产生的结果。事实上,气体温度与气体分子的平均动能(或平均速度平方)成正比。而熵则反映了气体分子运动的无序性,也就是分子的运动速度与分子所处位置的无关性。仙农的"信息熵"提出之后,人们进一步认识到,分子运动的"无序性"其实是一种"不确定性"。因此,"热学熵"与"信息熵"在某种意义上等价。于是"熵"把两门看上去完全不同的学科联系起来。

创立了现代电磁场理论的英国人麦克斯韦对于统计力学也有重要贡献。特别是,他于1871年提出了一个挑战热力学第二定律的"理想实验":

一个容器被分隔成A和B两部分,其中A充满了处于平衡状态的运动分子,B暂时为空;A,B之间有一个小孔连接,小孔边守卫着一个能够观察到分子运动速度的"小妖",它只允许A中速度较快的分子穿过小孔进入B。

如果确实有这样的"小妖"在起作用,那么,A部分的气体温

度将会逐渐降低，而B部分的气体温度则逐渐升高：处于热平衡状态的分子系统就会产生不平衡，系统的“熵”就会减小。热力学第二定律看来要失效。

然而，运用仙农提出的“信息熵”概念，能够合理地解释以上的“实验”：由于“小妖”提供了关于分子运动的额外信息，这使得系统分子运动分布的“不确定性”降低，也使得系统的“无序性”减少。也就是说，有没有“小妖”的系统是两个“熵值”不同的系统。而热力学第二定律只能适用于一个封闭系统。

4. 文字与二进制数码

由于仙农率先把信息量与二进制数的“位”联系起来，这就启发了人们把各种信息转化成二进制数的形式。

例如，作为文字信息数字化的基础，美国标准局(ANSI)于1968年公布了“美国标准信息交换码”(American standard code for information interchange，简称ASCII码)，其中包括了26个英文字母的数字化表示；中国国家标准局则于1980年了公布《信息交换用汉字编码字符集——基本集》(GB2312-80)，其中收录了6 763个简体汉字数字化表示；1995年，全国信息技术标准化技术委员会公布的《汉字内码扩展规范》(简称GBK)，收录了两万多个汉字的二进制数表示。

图像、声音和影视信息的数字化要比文字信息的数字化更困难。特别是影视信息，如果直接用二进制数来表示，那么产生的数据量之大，会给进一步处理和利用带来许多麻烦。为此人们设计出各种数据压缩技术，使影视信息的数字化数据量大大

减少。而数据压缩所依据的原理就是仙农提出的“信息熵”：因为一幅图像中以及两帧影视图像之间的数据存在明显的相关性，这说明全部数据的“不确定性”即“熵值”远非看上去那么高，所以能够在保持信息完整的同时，用少得多的二进制数来表示它们。

信息转化成二进制数之后，就可以让功能强大的电子计算机来处理，因为由无数的电子开关电路组成的计算机可以飞快地进行二进制数的运算；数字化信息能够通过通信网络传输，因为通信网络可以发送电子脉冲信号来传输二进制数；数字化信息能够储存在各种磁盘和光盘中，因为磁盘可以通过充消磁而光盘可以通过激光打洞来表示大量的二进制数。

当以上的一切都成为现实之后，信息时代（或叫做数字时代）就来临了。

5. 溯源于易经中的八卦

二进制数的有关历史　《易经》是我国最古老的一部历史文献，其起源可以追溯到大约5 000年前文字初创时期，传说中的伏羲“仰观天象，俯察地理”，发现了万事万物阴阳相生和相克的道理，而作八卦；其正式形成则是在3 000年前的周代，所以又称为《周易》。《易经》是一部卜筮之书，其中包含了上古时期中国社会和思想的丰富资料，对中国文化的影响极其深远。《周易》的卜筮方法是用“爻”：一个爻有两种形态：“阳”（用一长横划表示）和“阴”（用两短横划表示），三个爻放在一起，组成一个“卦”；因此总共有 $2^3=8$ 种卦（图 3-19）。



《易经》中的阳爻和阴爻

《易经》中的八卦

图 3-19

这八种卦再两两重叠，组成了六十四卦。卜筮者就可以用这六十四卦来解释万事万物，预测祸福吉凶。如果把阳爻当成“1”，把阴爻当成“0”，我们看到八卦可与 3 位二进制数对应，而六十四卦则对应于 6 位二进制数。因此，很多人认为，中国早已发明二进制数。当然，这种说法并不准确。由阴爻和阳爻组成的八卦是一套符号系统，被古人用来表示事物万象和原因。由 0 和 1 组成的二进制数现在也被用来表示各种信息。在这一点上，两者有类同之处。但二进制数是真正的数，可以对它进行各种严格和精确的数学运算；而八卦从来不是数，没有类似的数学性质。所以两者还是有根本不同的。

微积分发明者之一、德国数学家莱布尼茨(Gottfried Wilhelm von Leibniz，1646—1716)在 1679 年写了一篇题名“二进位数学”的文章，其中首次给出了关于二进制数及其运算的较完整描述，说明由 0 和 1 的排列形成的二进制数可以像十进制数那样表示任何整数。该文被认为是现代二进制数的肇始。莱布尼茨后来从到过中国的欧洲传教士那里了解到周易八卦，对其与二进制数之间的相似性惊叹不已。他花了许多精力，企图发现

《圣经》中上帝“七天创造世界”与八卦之间有何联系，希望以此来证明西方宗教和东方文化乃一脉相承。当然这已经是属于神学问题而不是科学问题了。

6. 2001 年平静地去世

1956 年，仙农被聘为 MIT 的教授，但仍在贝尔实验室兼职。他除了继续研究通信理论外，还研究人工智能，并取得一些成果。比如说，他制作了一个神奇的电子鼠，它能够自己学会如何从迷宫中走出来；他还设计了一个计算机下棋程序，被认为是该领域的一项突破性工作。



图 3-20　老年的仙农

1972 年，仙农从长期工作的贝尔实验室退休；1978 年，又从 MIT 退休。他的妻子原来是贝尔实验室的数据分析员，两人于 1949 年结婚，他们生有 3 个儿子和 1 个女儿。2001 年，他因患阿尔兹海默症而辞世。

因为创立了信息论，仙农被誉为“20 世纪最伟大的科学家之一”。他获得了无数的奖项，其中包括 1966 年获美国国家科学奖和 1978 年获日本京都奖；他同时是多家著名学术团体的会员。

未来之舟

仙农利用二进制数和概率论建立起了严格的信息论，结果不仅带来了信息时代。而且促进了信息的概念在其他学科领域中的应用，使得“信息”成为人类现代社会中最时髦的科技名词。

然而，就信息原来所具有的广泛意义来说，仙农的信息论存在着明显的

局限性。首先，仙农利用二进制数定义信息，这只适用于离散和有限可能的信息形式，如字母或文字；而现实中存在许多连续和无限可能的信息形式，如物体在空间中的位置和运动状态等，它们无法用二进制数来严格定义。

其次，仙农的信息论其实是一种通信论意义上的信息论，因为它只关心信息的表现形式和信息含量而不关心信息的内容和信息含义。但在许多情况下，后者甚至更重要。比如说，古人利用烽火台上的烟火之光来传递敌人来犯的信息；又如抗日战争时期，抗日军民用消息树来通报日本军队进庄。根据仙农的定义，烽火台或消息树只提供了 1 比特的信息。但这 1 比特信息可能关系到国家或村庄的生死存亡，远非开灯或关灯这种 1 比特信息所能比拟。

针对仙农信息论的不足，不同的学科根据各自的需要定义了不同的信息概念。如在图书馆学中，信息指的是书本中所包含的知识；在军事上，信息被称为情报，指的是关于敌方的情况及分析判断；在控制论中，信息则是指系统与外部世界所交换的内容；在企业生产、管理和市场营销中，也有各自的信息定义，等等。如何在数学的基础上，把所有不同的信息概念统一起来，形成一个更广泛的信息论学科，这是仙农以后的信息学家所面临的重要任务。

3.4 奠定机械自动化基础:维纳与他的控制论

就在仙农创立信息论的同一年，1948 年，维纳也创立了控制论。与此同时，冯·诺依曼提出的数字计算机方案问世，世界进入了信息时代。他们都是数学家。

1. 人类的梦想

机械自动化一直是人类的追求和梦想。传说中国古代西周时期，曾有一名叫偃师的巧匠为周穆王（约公元前 970 年）做了一个会歌舞和献媚的机械人；史载春秋时期，中国木匠鼻祖鲁班

（约公元前 507 年—公元前 444 年）曾经制作了能连飞三天的木头鸟、会拉车的木头马和能干活的木头人；《三国演义》中，诸葛亮（181—234）发明能运送粮草的木牛流马的故事让人津津乐道。在国外，据说公元前 2 世纪的古希腊人已造出了会开门和唱歌的机器人。当然，这些历史记载和传说极有可能只是古人将想象与现实混淆的产物。

事实上，直到 20 世纪 50 年代，人类才开始真正掌握了机械自动化理论和技术，从而有能力逐渐地把人类自古以来的梦想化为现实。经过了半个多世纪的发展，如今工厂里自动化生产流水线已司空见惯；无人驾驶的汽车、轮船和飞机也很平常。机械自动化的最高境界当然是制造能和人一样思考和行动的机器人。在这一方面同样取得了长足的进展。

1997 年，由美国国际商用机器公司（IBM）制造的电子计算机“深蓝”，以总分 3∶2 击败当时的国际象棋世界冠军、俄罗斯人卡斯帕罗夫（Gary Kasparov，1963—），成为该年的世界重大新闻。这标志着人造机器已经在一个曾经作为人类智慧象征的思维领域，超过了人类本身。与此同时，据统计全世界已经有大约 70 多万个怀有不同绝技的机器人，它们主要分布在工业和军事部门，代替人类从事着各种危险、繁重和复杂的工作。

人类究竟凭什么，竟能够制造出会像自己一样思考、行动和工作的机器？这要归功于一门博大精深的现代应用数学理论，那就是——“控制论”，它揭示了人和动物的行为奥秘，并奠定了机械自动化的理论和技术基础。

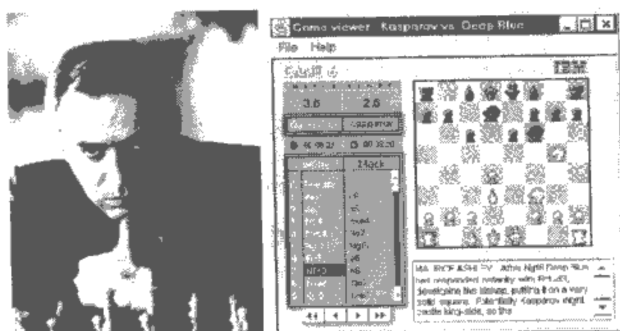


图 3-21　卡斯帕罗夫和“深蓝”的人机大战

2. 维纳从捡铅笔得到启示

1948 年，美国数学家维纳(Norbert Wiener，1894—1964)发表了他的划时代著作《控制论：或关于在动物和机器中控制和通讯的科学》，标志着控制论这门学科的正式诞生。其中“控制论”这一词的英文名称 Cybernetics，系维纳借用了希腊文单词 Κυβερνητηs(原意是指“舵手”和“管理”等)而自造，以表明这是一门崭新的学科。



图 3-22　维纳

维纳这部著作的内容极其广泛，以至看上去有点像在东拉西扯，却真实记录了控制论的思想是如何在实践中产生并发展起来的。书中不仅使用了群论、微分方程、数值计算、统计学、随机过程和信息论等数学工具，还涉及电子科学技术、通信论、计算机科学、生物学、医学生理学、社会学和哲学等学科知识。但始终围绕着一个核心概念，那就是——“反馈”。

维纳举了一个捡铅笔的例子。假定一个人要弯腰去捡地上

一支铅笔。为实现这一意图，他不需要、也不可能有意识地让身上每块肌肉有条不紊地进行必要的伸缩运动，以完成捡铅笔的动作。

实际上完成动作的方式会是这样的：当他有了捡铅笔的意图，其眼睛就会盯着地上的铅笔，身体肌肉会自然地进行相应的动作，让手接近铅笔，而眼睛随时通过神经向头脑汇报手与目标之间的误差，头脑命令肌肉调整运动，使手更靠近目标，直至捡到了铅笔。

这里，眼睛通过神经系统向头脑汇报手和铅笔的位置，就是一个"反馈"过程；它使得人能够有效地调节肌肉运动，不断地缩小误差，最后完成捡铅笔的动作。

这一简单的例子里包含了一个控制系统的基本要素，那就是：输入、对象或过程、输出、测量元件、反馈过程与控制器（图 3-23）。其中任何一个环节发生问题，都有可能影响系统实现其既定目标。例如维纳与他的同事发现，一些梅毒病患者因其脊髓神经受到破坏而影响了运动感觉信号的传递，即"输入"和"反馈"过程出现故障，导致出现"运动失调"症状，因而不能顺利地完成"捡铅笔"之类的动作。

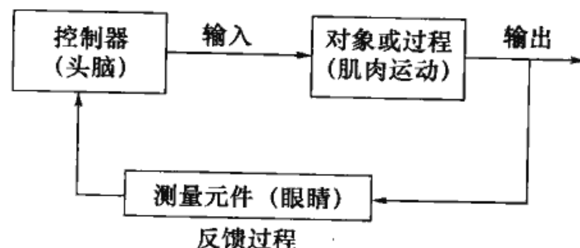


图 3-23　控制系统的基本结构图

人和动物的许多动作过程都可以通过这样的控制系统来描述。另一方面，如果系统中的各要素用机械装置来部分或全部实现，我们就得到了半自动化或全自动化的机械系统。比如说，维纳为美国军队设计的“防空火炮射击系统”就是一个半自动的控制系统，其控制对象是火炮，输出的是射向敌机的炮弹，测量元件是雷达和人眼的结合，反馈的信息是敌机的飞行轨迹及其与炮弹的最近距离，控制器则是一台微分运算分析机。

“反馈”机制对于一个控制系统中的重要性在于，它使系统保持了与外界的通信联系，并通过获得外界信息来有效地调整自己的行动。维纳在此引入了通信理论和信息论来研究反馈过程。由于在通信过程中会产生大量的干扰有效信息的噪声，维纳又提出了“滤波器”的机制，以过滤噪声。维纳还发现反馈量的过大或过小将会影响到系统目标的实现以及系统的稳定性。

反馈机制不仅能用于调节已知控制系统的行动，还可以用来预测未知系统的行为模式。因为从某种意义上讲，这种行为模式也是信息。比如说，维纳设计的“防空火炮射击系统”可以通过观察敌机不断地躲避炮火的动作来预测其将来的行为，从而提高炮火击中它的几率。为了能很好地完成预测的任务，维纳运用统计学和随机过程等知识，发展了从“时间序列”的数据中识别出所需信息的有效方法。

由此产生了控制论的另一个研究领域，那就是系统辨识：给定一个内部结构未知的控制系统——维纳称之为“黑箱”——要通过分析它的输入输出数据，来重建这一系统的结构，即要建一个有着相同的输入输出关系的“白箱”。系统辨识在现实生活中

有着广泛的应用。

反馈机制还可以使系统形成一种重要的能力，即学习的能力。因为所谓学习就是获取知识，而知识也是一种信息。维纳指出，学习能力是生命系统的特有的一种现象。但他设想可以让机器也具有学习的功能。他预见到可以设计一种下象棋的机器，它能够通过每次对局进行学习，不断提高自己的棋艺。维纳的预见现在已经实现。事实上目前许多计算机弈棋软件，包括前述战胜了国际象棋世界冠军的 IBM“深蓝”计算机所使用的软件，都具有很强的学习能力。

维纳就这样创建了控制论。这一理论已经在工业、军事、生物学、医学生理学、心理学、教育学和社会学等领域得到广泛的应用，并促使人类改变对世界和对人类本身的认识。

3. 机器人成为现实

由控制论带来的工业自动化能够使生产效率大幅度提高。例如，钢铁企业在实现了全面自动化后，可以使生产能力提高数倍到数十倍，生产人员大大减少；现代汽车制造几乎都已在自动化流水线上完成。而根据控制论原理制造出来的机器人已能够代替人类下煤矿开采，入深海作业，上火星探险。日本大阪煤气公司制作的机器人可以钻进煤气管道，检查煤气泄漏。美国科学家相信，人类不久将有能力运用纳米技术制造机器人，它甚至可以进入人体血管内，直接进行药物治疗或手术，等等。正如维纳所说的，工业自动化带来了第二次工业革命。

然而，维纳同时指出，新的工业革命是一把双刃刀，它可以

用来为人类造福，也可以毁灭人类。确实，自动化提高了工作效率，节省了人类的时间和精力，但它同时也带来了一系列问题。全面实行自动化是否会造成大规模的失业？那些因自动化而失去原有工作的人群将怎么安排？如果所有的事情都可以让机器人来做，而且做得比人还要好，那么人的存在还有什么意义？

特别是机器人与人类的关系问题，正在日益受到关注。如果机器人有了情感，并且有了自我意识，那么，它们是否该做人类合法的奴隶？还是允许它们与人类平等相处并享有“人”权？抑或它们竟会反过来，成为人类的主人？有关机器人与人类之间可能会有的各种关系，给科学幻想小说和电影带来了无穷的灵感和想象。一些以此为主题的电影，如《星球大战》、《终结者》以及《黑客帝国》等，曾经吸引了无数的观众。

幸好就目前来说，机械自动化所引起的失业问题还不是很严重。按照现在的科技水平，尚不可能造出思维和行动都全面胜过人类，而且带有情感和自我意识的机器人来。也许永远都做不到。即使有一天真的做到了，相信人类也会有足够的智慧来解决与机器人和谐相处、共同发展的问题。著名的科幻作家阿西莫夫(Isaac Asimov，1920—1992)，曾经在20世纪50年代提出过关于机器人行为的约法三章，即

(1)机器人不可伤害人类，或听凭人类被伤害而无动于衷；

(2)机器人必须服从人类的命令，除非该命令与第一条冲突；

(3)机器人必须保护自己的生存，只要这样做不与第一条或第二条冲突。

也许真的有一天，要为机器人如此立法。

4. 维纳创立控制论的清华渊源

维纳出生于一个崇尚教育和学习的犹太人家庭，其一生受父亲利奥·维纳（Leo Wiener，1862—1939）的影响很大。利奥出生于白俄罗斯，曾在波兰华沙大学医学院学习，后到德国柏林求学，不久又只身一人前往美国的新奥尔良，那时他年仅 18 岁。他在美国打过工，种过地，但一直没有放弃学习；最后竟当上了哈佛大学的斯拉夫语教授。利奥对其儿子维纳的教育倾注了很大的心血，有时甚至采取相当粗暴的方法，这给年幼的维纳带来心灵创伤，直到他长大成人也难以抹去。



图 3-24　少年维纳

然而总的来说，儿子并没有辜负父亲的期望。维纳从小就以神童著称，他三岁半就开始识字读书，七八岁时已经在大量阅读文学名著、科幻小说，以及包括物理学和生物学在内的各种科学著作；14 岁时从塔夫茨大学数学系毕业；而后到哈佛大学，先学动物学，又改学哲学和数理逻辑学，18 岁获哲学博士学位。

接着他远赴欧洲，先来到英国跟随著名的哲学家和数理逻辑学家罗素（Bertrand Russell，1872—1970）学习数理逻辑，同时跟随哈代（Godfrey Harold Hardy，1877—1947）进一步学习函数论和勒贝格积分；他又遵从罗素要求研读了爱因斯坦的相对论、卢瑟福的电子理论和波尔的学说。两年后去德国哥廷根大学，

跟随希尔伯特(David Hilbert,1862—1943)学习微分方程,并跟随兰道(Edmund Landau,1877—1938)学习群论。最后又回到罗素身边学习了一段时间。在欧洲的游学让年轻的维纳眼界大开,学问大长。特别是有幸受到罗素、哈代、希尔伯特和兰道这四位伟大数学家的言传身教,令他一生受益无穷。

1915 年回到美国后,维纳曾在哈佛大学讲授逻辑和哲学课,在这期间结识了一位特别要好的朋友,那就是年轻而富有才华的中国人赵元任。

维纳后来又当过一段时间的兵,还编辑过百科全书,最后经人介绍来到马萨诸塞理工学院(MIT)做数学教师,那是在 1919 年。他在 MIT 一直做到 1959 年退休,并继续担任荣誉教授。

1929 年,维纳打算为美国电话电报公司贝尔实验室研究"电路分析"的问题,为此他找到了 MIT 电气工程系的博士生李郁荣。两个人从此开始了长期的、卓有成效的合作。他们成功地设计出一种能够只允许特定信号通过的电气网络。其中已经蕴含了"滤波器"的概念,这对于维纳创建控制论有重要启发。他们后来为自己的设计申请了美国专利。维纳多次在各种场合,高度评价了李郁荣带给他的帮助。

李郁荣(Lee Yuk Wing,1904—1989),广东新会人,出生于澳门。1920 年在上海圣约翰大学读书。1924 年赴美国 MIT 电气工程系留学,先后获理学学士(1927 年)和硕士(1928 年)学位;1930 年,在维纳的指导下获得理学博士学位。



图 3-25 李郁荣

1932年,李郁荣回国;1934年,被聘为清华大学电机系教授。

1935年,在李郁荣的牵线搭桥之下,清华大学成功地邀请了维纳来电机系和算学系做访问教授。维纳在中国待了一年。他住在李郁荣的家里,除了上课之外,继续与李进行他们的合作研究,还学习汉语,有时下下围棋和五子棋。维纳对于他在中国的经历留下了美好的回忆。

抗日战争爆发后,李郁荣因战乱而失去了与已经南迁的清华大学的联系。后来经维纳介绍,再赴美国,回MIT电气工程系执教,直到1969年退休。

第二次世界大战期间,维纳致力于研究新式"防空火炮射击系统",所使用的主要控制设备是一种微分方程模拟分析计算机,这是他在MIT的同事、当时任美国政府科学主管的布什(Vannevar Bush,1890—1974)所发明的。维纳在研究中逐步形成了"系统辨识"的概念,这后来成为控制论中的一个重要研究领域。

维纳从中国回到美国后,与正在哈佛大学医学院访学的墨西哥医生与生理学家罗森伯吕特(Arturo Rosenblueth,1900—1970)也建立起了长期的研究合作关系。他们通过研究病人的运动失调的现象——比如说不能正常捡铅笔或拿茶杯——发现了人的头脑、神经、眼睛和肌肉之间所形成的控制、通信和反馈机制。这一发现后来成为维纳创建控制论的又一个关键环节。

维纳由于其个人天赋、家庭环境和社会机遇,而终于成长为一名知识渊博、研究领域极其广泛的杰出数学家。而他的工作经历,正好使他能够了解并掌握那些他后来创建控制论所需要

的专门知识。就好像命运已经安排好，要让他来完成这一将对人类的发展产生重要影响的开创性工作。

未来之舟

控制论自1948年正式创立以来一直在迅速发展，目前已经成为一门包含了多个分支领域的重要的应用数学学科。其主要分支包括：线性控制系统，非线性控制系统，最优控制理论，分布参数控制系统，系统辨识与过程参数估计，自适应、自学习、自组织的控制系统，随机控制与滤波，微分对策，大系统理论，生物控制论，模糊控制论，等等。从应用范围来看，与工业或物理过程有关的控制理论被称为“工程控制论”——在此领域，我国杰出的科学家钱学森（1911—）作出过重要的贡献。我国另一位科学家宋健（1931—）则在人口控制论领域中有开创性贡献。

3.5 数学哲学论战与计算机科学

数学一直被认为是人类知识体系中最严密、最精确和最可靠的学科。确实，从来没有发生过因为某条数学原理突然失效而造成桥梁倒塌或飞机坠毁的事件；当中学生做几何证明题或工程师解数学方程得到不正确的结果时，他们知道这肯定是由于自己的推理或计算有错误，而绝不会去怀疑数学本身。

但是，你可能不知道，关于数学基础的争论已经持续了两千多年；有时甚至争论得非常激烈。历史上许多最富有才智的数学家和哲学家曾投入这场争论。直至今天，争论尚未得出最后的结果。也就是说，虽然数学家已经建起了高耸入云的数学摩天大楼，但这座大楼的基础可能并不如你所想象的那样牢固。

然而，关于数学基础的争论并非毫无意义，它促进了数学和哲学思想的深入发展。特别是发生在20世纪初关于集合论的

争论，竟给人类带来了一个意外的副产品，那就是——计算机科学，它导致了第一台计算机的诞生，并使人类跨入了计算机时代。

1. 无理数带来的震撼

古人对于“数”有一种神秘主义的看法。比如说，中国春秋战国时期的哲学家老子(约公元前 600—公元前 500)曾经说过，“道生一，一生二，二生三，三生万物”。大约在同一时期，古希腊的早期数学家毕达格拉斯(Pythagoras，约公元前 580—公元前 500)则宣称“万物皆数”。古人所说的“数”一般是指正整数(或称自然数)，即 1，2，3，…

古人其实知道，除了整数之外，还存在别的“数”。例如，当几个小孩分一个苹果或一只西瓜时，就产生了“分数”；丈量两点之间的距离或计算土地面积时，得到的结果很可能也不是整数。但是，毕达哥拉斯及其门徒坚信，这些不是整数的数都是“可公度”的，即总可以表示成两个整数之比。

直到有一天，毕达哥拉斯的门徒发现了单位正方形的对角线长竟然是“不可公度”的。这一事实与其“万物皆数”的信念相违，令他们感到极度的惶恐不安。据说他们把首先发现这一事实的人推下了海，并且长期严守“存在不可公度数”的秘密。

数学小知识 关于单位正方形的对角线长不可公度的证明。根据勾股定理(古希腊人称之为毕达哥拉斯定理)，单位正方形的对角线长度是 $\sqrt{2}$ 。要证明 $\sqrt{2}$ 不能表示成两个整数之比。用反证法，假设 $\sqrt{2}=p/q$，其中 p,q 是两个互素的整数。

则易见，$2q^2=p^2$。于是，2 整除 p。这又推出 2 整除 q。于是 p,q 非互素，矛盾。证毕。



图 3-26　毕达哥拉斯

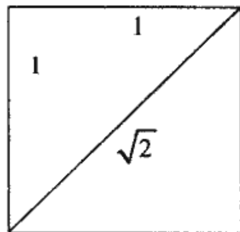


图 3-27

此次事件后来被称为“数学基础的第一次危机”。古希腊数学家因这次“危机”而发现了“无理数”，即“不可公度”的数。但是，他们并不承认无理数是数，而只称它为“量”。因为他们还没有能力建立起一个包括整数、分数和无理数的“实数”理论。这种理论直到 2000 年后才真正建成。

要把有理数(包括整数和分数)和无理数统一起来，这是一件极其困难的事。因为必须迈过一道难以跨越的坎，那就是——“无穷”。

2. 跨越“无穷”的门槛

古代数学主要研究有限范围内的数和量，并不直接与无穷打交道，不过它确实默认了一些无穷事物的存在。比如说，以下事实都被当作是无可置疑的：自然数有无穷多个；平面上分布有无数条直线，直线上有无数个点，直线的两端可以无限地延伸；时间和空间也是无限延伸的，并且可以无限分割，等等。中国古

代思想家庄子(约公元前 369 年—约公元前 286 年)曾经说,“一尺之棰,日取其半,万世不竭”。其中也蕴含了空间无限可分和时间能无限延长的思想。

然而,由于人类生活在有限的时-空范围内,所以他在实践中发展起来的自然语言和逻辑思维主要适用于有限的事物。当把这样的语言和思维用于无限的事物时,往往会得到一些看上去有悖常理的结论,即“悖论”。古希腊人芝诺(Zeno,约公元前 490—公元前 430 年)曾经提出一些著名的悖论,以下是其中的两个。



图 3-28　芝诺

阿基利斯追不上乌龟　阿基利斯是希腊神话中的英雄人物,以善跑著称;而乌龟当然是一个行动迟缓的动物。但芝诺的论证是,当阿基利斯要追赶已爬行了 n_1 米的乌龟,他首先必须也跑过这 n_1 米,而这时乌龟又爬行了 n_2 米,等他跑过这 n_2 米,乌龟又爬了 n_3 米……这样的过程永远不会完结,所以阿基利斯永远追不上乌龟。

飞矢不动　按照芝诺的说法,因为飞行的箭在时间的任意一刻只能有一个空间位置而不可能同时占有两个空间位置,因此它在任意一刻是不动的,也就说它没有任何的移动时间,由此可知它应该始终保持静止。

芝诺的这两个悖论均与空间和时间的无限可分性有关。它们显示了,当人类的思维对象涉及无穷的事物和过程时,将可能遇到怎样的逻辑困难。

17 世纪，牛顿和莱布尼茨发明了微积分，从而开创了近代数学的历史。运用微积分方法，能够方便地求解许多曲边形或曲面体的几何量，并能有效地处理各种变速运动的问题，使得数学研究领域大大扩展。然而，微积分的本质就是“无穷的算术”，即它把无穷小和无穷大都当作普通的数和量，对其施以加减乘除等种种运算。于是，微积分在给数学带来一场革命的同时，也不可避免地带来了与无穷有关的逻辑悖论和矛盾。

例如，牛顿为了求面积方程 $z=ax^m$ 的变化率，他先设 x 有一个无穷小增量 o，并计算 $\frac{a(x+o)^m-ax^m}{o}$，再令 $o=0$，从而得到变化率方程 $y=max^{m-1}$（图 3-29）。

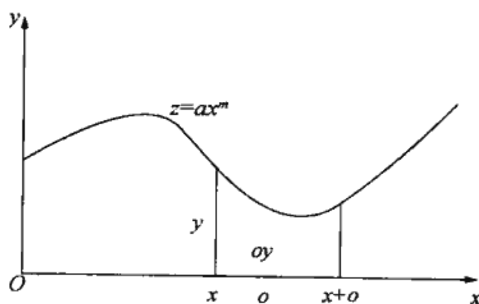


图 3-29


图 3-30　贝克莱主教

18 世纪的英国主教贝克莱（George Berkeley，1685—1753）严厉批评了牛顿的这种做法。他说增量 o 一会儿是零一会儿不是零，自相矛盾。对于以形如 $\frac{0}{0}$ 的表达式给出的变化率，他讥讽道：“它们既不是有限量也不是无穷小量更不是虚无……我们是否可称它们为消失了量的鬼魂？”

贝克莱的攻击让当时的数学家无回手之力。

此次事件因而被称为关于数学基础的第二次危机。但是数学家并没有因此而放弃微积分，而是继续积极地运用它来开拓新的数学领域。事实上，18—19 世纪正是微积分学蓬勃发展的最辉煌时期。

3. 集合论悖论的出现

其实，18—19 世纪的数学家并没有停止为数学建立牢固的逻辑基础的努力。这些努力以德国数学家康托（G. Cantor，1845—1918）于 19 世纪下半叶创立了集合论而达到顶峰。按照康托的说法：

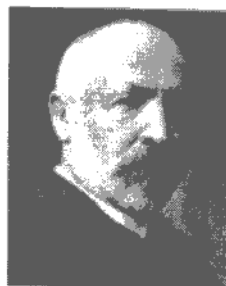


图 3-31　康托

一个集合就是一组确定的、可彼此区分的对象，这些对象是人们直觉和思维的产物，它们被称为是该集合中的元素。

康托运用集合论，把无理数定义为以有理数为元素的基本序列，这样就建立起了严格的实数理论，从而彻底解决了第一次数学危机。而在集合论基础上建立的 ϵ-δ 语言，可以把微积分中关于无穷量的运算严格定义为一个极限过程；于是贝克莱主教的指责不再成立，第二次数学危机也得以化解。

康托甚至在集合论的基础上建立起了超限数理论，即关于无穷集合的大小、分类和排序的理论，得到一些奇妙的结论。比如说，他证明了所有有理数的集合 **Q** 和所有自然数的集合 **N** 一样大（即 **Q** 中的元素可以和 **N** 中的元素建立起一一对应）；但所有实数的集合 **R** 要比集合 **N** 大。康托进而猜测：不存在比 **R** 小

但比 N 大的集合。这就是著名的“连续统猜想”，是迄今为止尚未被解决的数学难题。

看来康托已成功地为数学建立起了牢固的基础，使得数学家们可以放心地继续营造数学大厦了。事实上，康托以后的整个现代数学的发展，都建立在集合论的基础上。数学家们对于康托的工作极尽赞美之词，称其为“数学精神最令人惊羡的花朵，人类理智活动最漂亮的成果”；“可能是这个时代所能夸耀的最伟大的工作”。

但是，好景不长。1901 年，英国数学家和哲学家罗素（Bertrand Russell，1872—1970）发现了一个关于康托集合论的悖论，令众人目瞪口呆。他的悖论是这样的。



图 3-32　罗素

罗素悖论　把所有的集合分为两类：第一类的集合包含自身为元素，第二类的集合则不包含自身。现令 M 是以所有第二类集合为元素的集合，问 M 为第一类集合还是第二类集合？如果 M 属于第一类，则 M 包含了自身为元素，但根据 M 的定义，M 中所有的元素都属于第二类集合，因此 M 必须属于第二类，矛盾；如果 M 属于第二类集合，则根据 M 的定义，M 本身属于 M，于是 M 又必须属于第一类，矛盾。

罗素后来把他的悖论通俗化为以下的“理发师悖论”。

理发师悖论　一位乡村理发师宣称要给村上所有自己不刮脸的男子刮脸，但不会给自己刮脸的男子刮脸。有一天，他发生

了疑问：他是否应当给自己刮脸？如果自己刮脸的话，则按照前面的声明他就不能给自己刮；如果自己不刮脸的话，按照声明他又必须给自己刮。

后来又发现了其他的悖论。这些悖论给予康托的集合论以沉重的打击。数学家们感到愕然：已加固的数学基础似乎出现了更大的裂缝！人们称这是“第三次数学危机”。

然而，数学家们并不想放弃康托的集合论。德国大数学家希尔伯特(David Hilbert，1862—1943)说道，“没有人能够把我们从康托所创造的乐园中赶走。”希尔伯特提出了一个使集合论避免悖论的方案——后被称为“希尔伯特纲领”。该纲领的要点是：按照欧几里得几何的模式，构建一个公理化的集合论体系，并利用可构造的方法，证明该体系是完备的(即关于数学的所有论断都能够在其中得到证明或证否)和相容的(即其中不会推出两个互相矛盾的数学论断)。

希尔伯特纲领看起来很合理，如果能实现的话，那就一劳永逸地解决了数学基础的问题。但是在1931年，年仅25岁的奥地利青年数学家哥德尔(Kurt Gödel，1906—1978)证明了一个真正惊人的定理：任何一个包含了自然数的集合论公理化系统不可能既是完备的又是相容的——也就是说，如果这个系统是完备的，那它肯定不相容；如果它是相容的，那肯定不完备。这个定理被称为“哥德尔不完备定理”，它彻底粉碎了希尔伯特纲领。

哥德尔不完备定理等于在明确宣告：关于数学基础的问题不可能在数学的框架下得到彻底解决。对此，数学家们并不感

到沮丧，反而像得到了解脱，从此不再关心数学基础问题，而是专心致志地在康托集合论的基础上继续发展现代数学。著名数学家冯·诺依曼赞誉哥德尔的成就“是独一无二的，是一座丰碑——甚至超过丰碑。”



图 3-33　希尔伯特



图 3-34　哥德尔

但在另一方面，罗素和希尔伯特等人为解决数学基础问题而做的努力也没有白费。在他们工作的基础上形成了“数理逻辑学”和“元数学”等新数学分支，为以后计算机科学的创立和发展提供了充分的思想和理论准备。

4. 计算机科学的诞生

所谓“希尔伯特判定问题”引申于“希尔伯特纲领”。它问：“对于任意一个数学命题，是否存在一种算法能够判断该命题可证或不可证?”1936 年，24 岁的英国青年数学家图灵发表了论文“论可计算数及其在判定问题中的应用”，给出了该问题的一个解答。然而，此篇论文的意义远远超过了解答问题的本身。图灵在文中提出了“通用计算机”(后来被称为“图灵机”)的概念，并定义“可计算数”为可由图灵机用“0”,“1”符号表示成二进制序列的实数。图灵进而说明，所

有的“可判定问题”和“可计算问题”都可以容易地表示成“可计算数”的问题。在此基础上他给出了希尔伯特判定问题的否定回答。

数学小知识　图灵机是一种理想的自动机，它由一条单边无限长的线性方格带和一个具有若干不同状态的读写头组成；读写头每次注视带上的一个方格，并根据自身的状态和被注视方格上的符号执行以下 5 种动作之一：(1)左移一格，(2)右移一格，(3)在被注视格上写符号，(4)把被注视格上的符号擦掉，(5)改变自身所处的状态。

图灵机不仅立即成为研究“可计算问题”的一个关键工具，它甚至成为 10 年以后才制造出来的真正计算机的逻辑原型。因而，图灵的论文被认为开创了现代计算机理论科学。

1945 年，美籍数学家冯·诺依曼为美国军方的“弹道研究实验室”设计了一台叫做 EDVAC 的计算机（全称 electronic discrete variable automatic computer，电子离散变量自动计算机）。EDVAC 由五个部分组成：运算器、控制器、储存器、输入和输出装置；其中的指令和数据均以二进制形式存储；控制器从储存器调用指令，并根据指令自动执行运算、输出（打印）结果、输入新数据、调用新指令等操作。可以看出，其工作原理与图灵机很相似，例如均采用二进制数，均将指令当作数据一样处理，计算机工作时先把指令储存起来，然后一条一条地调用并执行，就这样自动运行下去。

由于种种原因，EDVAC 直到 1951 年才得以建成使用。自此以后，计算机技术开始以令人难以想象的速度飞快发展；但是迄今为止，几乎所有的计算机仍然是按照 EDVAC 的结构——被称为“冯·诺依曼结构”——建造的。因此，冯·诺依曼被公

认为现代计算机之父。

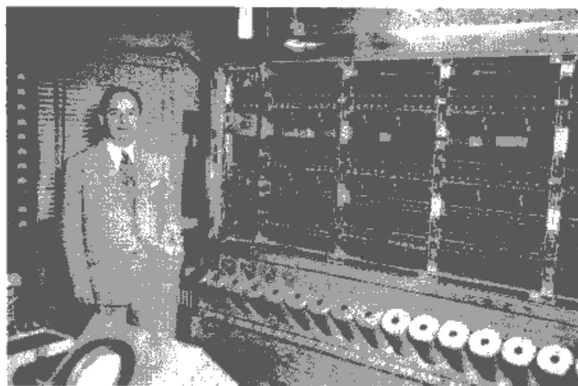


图 3-35　冯·诺依曼与他所设计的计算机

在 EDVAC 之前，美国军方的另一台计算机 ENIAC（全称 electronic numerical integrator and computer，电子数值积分计算机）已于 1946 年问世，它被称为世界上第一台电子计算机。其实，ENIAC 在设计和建造过程中也得到过冯·诺依曼的重要帮助。不过，它采用十进制数，而且不是指令储存的工作方式。因此严格地讲，ENIAC 并不是现代意义的计算机。但在另一方面，可以证明 ENIAC 也与图灵机等价，即它们所能完成的计算任务是一样的。



图 3-36　ENIAC 被认为是世界上第一台电子计算机

冯·诺依曼(John von Neumann,1903—1957)出生于匈牙利布达佩斯的一个犹太人家庭,父亲是银行家。和另一位美国数学家维纳(参见 3.4 节)一样,冯·诺依曼小时候也是有名的神童,熟练掌握多国语言,并且酷爱读书和学习。20 多岁时,冯·诺依曼已经是世界著名的数学家。1933 年,美国普林斯顿高级研究所从欧洲聘请了三位最杰出的科学家作为终身教授,他们就是爱因斯坦、外尔和冯·诺依曼。该研究所很快成为世界数学中心。

冯·诺依曼也曾经研究过数学基础和集合论,并且获得不少重要结果。1931 年,哥德尔发表了他的"不完备定理"。冯·诺依曼在对哥德尔的成就表示极度钦佩的同时,因知道数学基础的问题已不可能得到彻底解决而转向其他研究领域。但他对数理逻辑和元数学的深刻了解,无疑是他后来能够在计算机科学领域做出开创性工作的一个关键原因。

冯·诺依曼的数学贡献极为广泛。比如说,在纯粹数学领域,他的贡献遍及集合论基础、测度论和泛函分析,并创立了算子代数;在应用数学领域,他的研究包括计算机理论、数值计算、流体力学等,并创立了博弈论(参见 1.9 节)。另外,第二次世界大战期间,他还在美国研制原子弹工程——曼哈顿计划——中发挥了重要的作用。

5."图灵测验"与人工智能

图灵(Alan Mathison Turing,1912—1954)出生于英国伦敦的一个中产阶级家庭。父亲曾在印度马德拉斯邦政府机构中工

作，母亲则是马德拉斯铁路局总工程师的女儿。图灵1931年进剑桥大学国王学院，学习量子力学、数理逻辑和概率论，1935年以优异成绩毕业留校做研究员。1936年发表了"论可计算数及其在判定问题中的应用"的开创性论文后，图灵赴美国普林斯顿大学深造，并于1938年获得博士学位。他谢绝了留下来做冯·诺依曼助手的邀请，回到英国。



图3-37　图灵

图灵回国后不久，第二次世界大战爆发。图灵立即被政府征召，投入到破译德军"隐谜"密码的"超级机密"工作中。图灵在这条看不见的战线上发挥了至关重要的作用，为盟军赢得反法西斯战争作出了巨大贡献(详见3.2节)。

第二次世界大战结束后。1945—1947年，图灵在英国国家物理实验室工作，继续研究计算机理论。1948年，他来到曼彻斯特大学，担任大学计算实验室副主任。1950年，图灵发表了论文"计算机与智能"，这是影响计算机科学发展的又一篇里程碑式的论文。

图灵在文章中深入探讨了计算机是否会"思考"的问题。虽然那时电子计算机问世不久，图灵却大胆预测：再过50年，计算机可能会具有与人不相上下的智力。他提出了一个检验计算机是否具有与人相当思维能力的著名方法，被称为"图灵测验"：由一个提问者向被分别隔离开来的两受问者提问，其中一个是人，而另一个是一台计算机。如果提问者无法通过问答来确定受问

者中哪一个是人和哪一个是计算机，则认为此计算机已具备了和人一样的思维能力。

图灵由此开创了人工智能的研究。在图灵发表论文的 50 多年之后，计算机技术有了突飞猛进的发展。如今，计算机已能够在国际象棋较量中轻而易举地击败人类世界冠军。因此可以说，在有些智力领域，确实如图灵所料，计算机已具备与人相当甚至超过人的能力。不过总的说来，还没有一台计算机能够通过图灵测验，即使是运算速度达到每秒数百万亿次的最新型超级计算机也做不到。也许还要再过 50 年，计算机才能达到如此水平。

1952 年，图灵因同性恋事发被判有罪，被剥夺了从事国家机密工作的权利。1954 年，图灵因氰化钾中毒而英年身亡。

为了纪念图灵对计算机科学奠基性的贡献，美国计算机协会于 1966 年设立了“图灵奖”；该奖被认为是计算机科学领域中的诺贝尔奖。2000 年的获奖者是曾任普林斯顿大学计算机系教授的华人科学家姚期智(1946—)。

2001 年 6 月 23 日，一座图灵的雕像在英国曼彻斯特市的萨克维里公园落成。2004 年夏，曼彻斯特大学成立了“阿兰 · 图灵研究所”，该研究所的目标是要成为以数学为核心的新学科研究的世界中心。

未来之舟

哥德尔不完备定理不仅事实上终结了人们关于数学基础问题的争论，还对哲学中认识论和本体论的研究产生了深远的影响。罗素和希尔伯特等人关于数学基础的工作虽然因哥德尔不完备定理而告失败，却为图灵和冯 · 诺依曼开创计算机科学创造了条件。而图灵的工作还导致产生了另

外两个新学科，那就是可计算性理论和人工智能研究。

图灵首先提出了计算机的工作原理，冯·诺依曼将该原理实现，仙农奠定了计算机信息处理的理论基础，维纳阐明了信息-行为的互相作用机制。由于这四位20世纪最富有创造力的数学家的工作，使人类进入了计算机时代、信息时代和自动化时代。

图灵-冯·诺依曼计算机的工作特点是串行处理，即计算机依次一条一条地执行指令。这种计算机工作方式一直被沿用至今。但与此同时，为了加快运算速度和提高计算机资源的利用效率，计算机专家从20世纪70年代开始研究并行计算，即让计算机同时执行多条指令。目前并行计算原理已被用于多处理器计算机的制造，以及多台计算机联合工作的设计中。

3.6 数学证明的机械化之路

一般认为，数学证明是头脑思维的产物。“灵机一动，计上心来”。这似乎和机械的死板运算不相干。但是，计算机固然不能代替人的头脑，但是一部分繁重的“按部就班”式的脑力劳动，还是应该交给机器去做。人类在20世纪取得了一些进展，其中包括吴文俊的创新研究。

1. 从数值计算谈起

学习和研究数学的任务可以分为两大类：证明数学命题和解数学方程。像“三角形的内角之和等于180°”，“三角形的高相交于一点”和勾股定理等，都是典型的数学命题，我们在中学里就已经学会证明它们了。费马大定理、高斯-博内定理和庞加莱定理等，则是非常困难的数学命题，经过几代数学家的努力才得以证明。至于哥德巴赫猜想和黎曼猜想等数学命题，迄今尚未

能证明。

数学方程包括代数方程、微分方程、积分方程和差分方程等。例如

$$ax^2 + bx + c = 0 \tag{1}$$

就是一个简单的一元二次代数方程。当然，工程师和数学家所研究的方程要复杂得多。

解数学方程通常有两种方法。一种叫做解析法，即设法求出满足方程的未知量的解析表达式，这些表达式通常是方程中各项系数的函数。如中学里已教过，方程(1)的解析解为

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}。$$

解析方法的优点在于：它所求出的一般是该类方程的通解，并且是没有误差的精确解；还可以通过解析表达式深入研究这些解的结构和性质。任何数学方程，如果能够写出其解的解析表达式，那就相当于已经彻底掌握这种方程了。可惜的是，只有很少种类的数学方程适用于解析方法。即使是最简单的一元代数方程，阿贝尔和伽罗瓦早在两百年前就已经证明，当其次数大于 4 时是没有一般根式解的。

另一种解数学方程的方法叫做数值法，即设法获得方程的数值解。通常是用十进制数或二进制数表达的近似解，一般通过迭代逼近获得。如对于一元二次方程(1)，可以运用“切线法”，写出其迭代方程式

$$x_{n+1} = x_n - (ax_n^2 + bx_n + c) / (2ax_n + b)。 \tag{2}$$

假设方程(1)中的 $a=1, b=-1, c=-1$，则有

$$x^2 - x - 1 = 0。 \tag{3}$$

我们令 $x_0=0$，然后用方程(2)迭代计算得到

$$x_1=-1, x_2=-0.666\,666\,667, x_3=-0.619\,047\,619,$$

$$x_4=-0.618\,034\,448, x_5=-0.618\,033\,989。$$

于是，仅通过 5 次迭代就已经得到了方程(3)的精确到小数点第 9 位的数值解。

数值法的一大优点是，它能够解出大部分数学方程，尤其适用于求解复杂的方程。比如说，2 000 多年以前中国古代数学名著《九章算术》中，就已经有了求平方根和立方根数值解的机械算法“开方术”和“开立方术”。在此基础上，北宋的贾宪(活动于约 1050 年)发明了“增乘开方法”(其中要用到著名的“贾宪三角”)，南宋的秦九韶(1202—1262)发明了“正负开方术”。这些都是求高次方程数值解的机械算法——从理论上讲，可以用它们求出任意高次方程根的数值解。作为对比，前述“解析法”最多只能求出 4 次方程的根。

然而，数值法的最大优点在于，它其实是一种机械的解题方法，因此可以通过计算机来实现。事实上，人类一开始建造计算机的目的就是为了数值计算。1946 年问世的第一台电子计算机 ENIAC，其全称是“电子数值积分计算机”。后来，计算机才被越来越多地用于信息处理。不过，随着科学技术的发展，对数值计算的需求也在快速增长。如卫星上天，天气预报，建造大坝，设计飞机，模拟飞行，生产新药等，都需要进行大量的计算。为此人们不惜花费巨资建造速度越来越快的“超级计算机”。由美国 IBM 公司在 2006 年制造的“蓝色基因”(图 3-43)，是目前世界上运算速度最快的超级计算机，其运算速度达到每秒 380 万亿次，

它主要用于模拟分子生物学现象的数值计算。

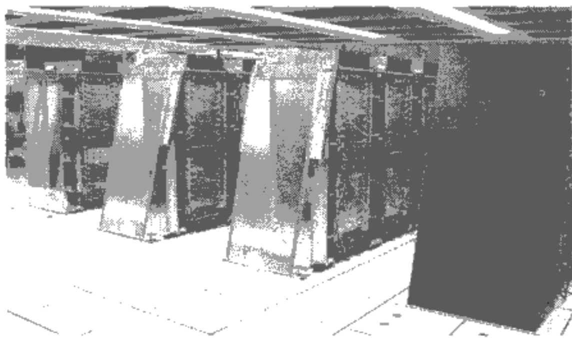


图 3-38　超级计算机——“蓝色基因”

鉴于数值计算在人类生产劳动和科学研究中占据越来越重要的地位，许多数学家认为，依赖于计算机的机械化数值计算方法将成为数学研究的主流。他们的看法并非毫无道理。

现在回首来看数学研究的另一大任务——数学命题证明。人们不禁要问：数学证明是否也能实现像数值计算那样的机械化，从而也可以通过计算机来完成？

2. 逻辑推理的机械化

关于推理证明的机械化尝试，可以追溯到 17 世纪德国数学家和哲学家莱布尼茨(Gottfried Wilhelm von Leibniz, 1646—1716)。这位兴趣广泛的古今闻名大学者在 20 岁时就发表了一部题名《组合的艺术：把所有关于真理的推理归结为一种演算的通用方法》的著作，其中试图通过把复杂的概念分解为一些简单概念符号的组合，来建



图 3-39　莱布尼茨

立起一个符号化的推理演算体系。莱布尼茨设想有了这样一种能表示所有的思想和概念的“普遍符号语言”体系，人们就不必为了一些信念和理论而徒劳地费尽口舌地争论不休了。到那时，只需争论的各方都拿出纸和笔，说：“让我们来演算一下，看看究竟谁对谁错。”就像解决数学问题一样。莱布尼茨一生致力于建立这样的体系，但并没有完成。

200 年以后，英国数学家布尔(George Boole，1815—1864)发表了著作《作为数学逻辑和概率理论基础的思想规律研究》(1854 年)。其中，他用“×”、“+”和“−”这些原来的数学四则运算符号，来表示逻辑运算“与”、“或”和“非”；并用数字“1”和“0”来表示命题的“真”和“假”；运用这些符号，他把复杂的命题分解为一些简单的基本命题的逻辑组合，而命题的真假则可归结为组成它的那些基本命题的真假情况。就这样，布尔创立了关于命题演算的符号化系统，后被称为“布尔代数”。这是朝着莱布尼茨的目标前进了一大步。布尔代数后来在数字电路技术、通信论和信息论中也有广泛的应用。



图 3-40　布尔

到了 20 世纪初，由于康托的集合论出现了悖论，使得一些数学家决心接受莱布尼茨的想法，要在布尔代数的基础上为数学建立起一个完整的符号语言体系，以求一劳永逸地彻底摆脱因自然语言的缺陷而产生的种种逻辑困难。在这一方面，罗素和希尔伯特以及他们的追随者作出了重要贡献。

罗素认为，数学归根结底就是从前提到结论的一种逻辑推理，因此我们应该建立一个符号化的逻辑系统，并设法把数学纳入其中。罗素的这种观点被称为“逻辑主义”。他和怀特海（Alfred North Whitehead，1861—1947）合著的三卷本巨著《数学原理》（*Principia Mathematica*，1910—1913），集中体现了逻辑主义的思想。

希尔伯特则认为，我们只需建立一个形式化的数学公理系统，并且证明这样的系统是完备的和相容的。希尔伯特的观点被称为“形式主义”。他和阿克曼（Wilhelm Ackermann，1896—1962）合著的《理论逻辑原理》（*Grundzüge der theoretischen Logik*，1928），是形式主义的经典著作。

表面上看，罗素逻辑主义和希尔伯特形式主义的主张并不相同，而且这两个学派之间曾经有激烈的争论，其实他们做的是同样的事，而且相互之间还借用了不少概念和符号。虽然因为“哥德尔不完备定理”（1931）而宣告了罗素和希尔伯特所声称的目标都注定不能达到，但是他们确实为我们留下了一个能表述相当一部分数学命题的形式化语言体系。例如，著名的哥德巴赫猜想说：任意一个大于2的偶数都能够表为两个素数之和。这可以用形式化的语言表达如下，

$$(\forall x \in \mathbf{N})2 \mid x \cap x > 2 \rightarrow (\exists p \in \mathbf{N})(\exists q \in \mathbf{N})$$
$$(\forall y \in \mathbf{N})(y \mid p \rightarrow y = 1 \cup y = p) \cap (\forall z \in \mathbf{N})$$
$$(z \mid q \rightarrow z = 1 \cup y = q) \cap x = p + q。$$

其中 $\forall$ 可解释为“任意的”，$\exists$ 解释为“存在”，$\in$ 解释为“属于”，$\mathbf{N}$ 表示自然数集合，$\cap$ 和 $\cup$ 分别表示逻辑算符“与”和“或”

(相当于前述布尔代数中使用的“×”和“+”符号),→ 表示“蕴含”,|表示“整除”。

于是,数学的符号化(形式化)体系已经大体建成。莱布尼茨的理想得到了部分实现。下一步的目标,应该是研究如何在形式化数学体系中实现机械化推理,从而能够让计算机自动完成数学证明。但要达到这一目标,还有很漫长的路要走。

3. 机器证明的前进脚步

计算机数学证明的首次尝试,始于美国卡内基梅隆大学的计算机与心理学教授西蒙(Herbert Simon,1916—2001)与兰德公司的数学家和计算机专家纽厄尔(Allen Newell,1927—1992)和肖(John Cliff Shaw,1922—1991)的合作。他们三人于 1956 年研制了一套叫做“逻辑理论机”(logical theory machine,简记 LTM)的计算机程序,并运用该程序试图证明罗素和怀特海合作的名著《数学原理》中开头 52 条定理,结果成功证明了其中的 38 条。LTM 程序使用的证明方法是模拟人类思维方式的“试探法”,这种方法的优点是适用范围广,如它还可以用于发现化学和物理学定律,建立决策系统和实现计算机弈棋等。

LTM 是第一套有实用意义的人工智能领域中的计算机软件,它对以后人工智能研究的发展有相当大的影响。它的发明者中的两位——西蒙和纽厄尔——后被称为人工智能符号主义学派的创始人;因为他们试图用《原理》中所阐述的符号化数理逻辑系统,建立起人工智能的理论。1975 年,西蒙和纽厄尔因“在人工智能和人类认知心理学等领域的基础贡献”而荣获由美

国计算机协会颁发的图灵奖。顺便提一下，西蒙还由于“在经济组织中决策过程的开创性研究”而在 1978 年获得诺贝尔经济学奖。



图 3-41 西蒙(左)和纽厄尔(右)在研究计算机弈棋

基于“试探法”的 LTM 程序虽然有较广泛的应用，但它的实际推理能力并不强，速度也不快。两年后，美国哈佛大学的数理逻辑教授王浩(1921—1995)取得了更好的结果。

1958 年夏天，王浩用计算机汇编语言编写了三个数学证明程序，并在 IBM704 型计算机上运行。其中第一个程序用于证明《数学原理》前五章中关于命题演算的 200 多个定理，结果在 37 分钟内完成。如果去除数据输入输出时间，计算机实际运行不到 3 分钟。第二个程序要求计算机形成新的命题，并从中挑选出非平凡的。结果在 1 小时内构建并证明了14 000条命题，并选出1 000多条较有意义的定理。



图 3-42 王浩

第三个程序处理带等式的谓词演算。结果在1小时内证明了《原理》后五章中带等式谓词演算的150多条定理中的120多条。一年后，王浩用改进的程序，只花8.4分钟就证明了《原理》中带等式谓词演算的全部350多条定理。

作为比较，用西蒙等人设计的LTM程序证明《原理》中的定理2.45用了12分钟，证明定理2.31运行23分钟后仍无结论。而用王浩的程序，证明这两条定理分别只用了3秒和6秒钟。

王浩的证明方法大致是这样的：因为《原理》中的定理公式大都是用形式化语言写成的符号序列，王浩通过巧妙地逐步消除这些符号序列中的逻辑算符（即前述的"∩"和"∪"等符号），使得公式不断地简化，最后形成证明。

在取得了这一系列重要成果之后，王浩郑重宣布：建立数理逻辑学应用新分支的时机已到，这个新分支可称为"推理分析"，它对于数学证明的作用就像数值法对于解数学方程；相信它在不久的将来能够使计算机证明困难的新数学定理。

王浩因其在数学机械证明领域中的开创性贡献，而于1983年荣获由人工智能国际联合会与美国数学会联合颁发的"里程碑奖"（Milestone Prize）。

王浩出生于山东济南，父亲是中学教师。王浩从小就喜爱哲学和逻辑。1939年考入西南联大数学系，学习期间经常到哲学系听课。1946年考入美国哈佛大学哲学系，毕业后曾到欧洲的瑞士苏黎世工业大学和英国牛津大学等处做研究和讲学；回到美国后，又先后在哈佛大学和洛克菲勒大学任教授。王浩在哲学、数理逻辑学和计算机科学等领域作出了一系列重要的贡

献：除了计算机证明外，还包括改进形式化公理系统，提出关于图灵机的新理论，以及证明了一类逻辑公式的不可判定性，等等。王浩和著名逻辑学家哥德尔交往甚密，他后来把两人之间的谈话内容编写成著作出版。

王浩是祖国的海外赤子。20 世纪 50 年代，他打算多掌握一些有实用性的知识，以便回国效力，于是开始学习刚刚兴起的计算机理论。结果没多久，他就在计算机证明中取得了开创性的成就。后因种种原因，直到 1972 年，他才得以回国讲学。王浩后来在海外多次撰文，赞扬新中国所取得的种种成就。

4. 吴文俊独辟蹊径

客观地讲，在罗素的《数学原理》中所演绎的，是一种建立在符号逻辑基础上的形式化的数学，与实际的数学有区别。所以说，王浩利用计算机所证明的，大多是形式化数学的定理。要让计算机证明真正的数学定理，还需要克服许多困难。

中学生都体会到，初等几何的证明是对智力的一大挑战。欧几里得《几何原理》中的第五个命题“等腰三角形的两底角相等”，被西方人称为“笨人难过的桥”。意思说，只有学会证明这个基本命题，才有可能学好几何。而初等几何证明当然是所有数学证明中最简单最基本的任务了。因此也可以把初等几何证明当作计算机的“笨人难过的桥”。要使计算机能够证明真正的数学命题，必须让它先过这座“桥”。

1977 年，中国数学家吴文俊发表了开拓性论文“初等几何判定问题与机械化证明”；1984 年，他又出版了专著《几何定理机器

证明的基本原理》。在这些文献中，吴文俊提出了实现几何定理机械化证明的一种崭新的方法——国际上称为“吴方法”。

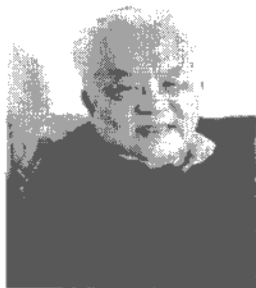


图 3-43　吴文俊

“吴方法”实现几何定理机械证明的大致步骤：

先把几何命题中所给出的条件和所要证明的结论都化为一些代数方程；接着把命题条件所对应的那些方程“整序”成一种升列结构（吴文俊证明这样的整序总能够完成），称为“特征列”；然后求命题结论所对应方程对于特征列的余式。如果余式为零，则证明了命题为真；如果余式不等于零，则证明了命题为假。

通过计算机使用“吴方法”，能够证明大量不平凡的几何定理，甚至包括那些人们很难证明的定理，还发现了一些人们以前不知道的新定理。于是，由于吴文俊的开创性贡献，终于使得计算机数学证明的发展通过了“几何证明”这座桥。而吴文俊本人也因此成为引领国际数学机械化证明发展潮流的带头人。在他的领导下，一批中国数学家在这一领域中不断获得重要的成果。如今，数学机械化证明已能够包括非欧几何、三角函数、超越函数、不等式和微分几何中的定理。

吴文俊 1919 年生于上海，1940 年毕业于上海交通大学数学系，1949 年获法国国家博士学位，1951 年回国，任北京大学数学系教授。吴文俊主要研究拓扑学。1956 年，因示性类及示嵌类的工作荣获国家第一届自然科学奖一等奖（其他两位一等奖获得者为华罗庚和钱学森），1957 年成为最年轻的中国科学院

院士。

从 1976 年开始，吴文俊开始对中国数学史感兴趣。他发现中国古代数学家重视找到解决数学问题的机械化程序，而不太关注数学的演绎和推理。于是从中受到启发。他认为现代数学也应该走这样的道路，即不管是数学计算还是数学证明，都应该致力于找到适当的机械化程序，从而能够借助于越来越强大的计算机来解决问题。于是，他开始研究初等几何的机械化证明，很快就取得了突破。

吴文俊因对于拓扑学的重要贡献和在数学机械化证明领域中的开创性成就，而获得了国际国内一系列学术大奖；包括第三世界科学院数学奖(1992 年)，陈嘉庚数理科学奖(1993 年)，香港求是基金会“杰出科学家奖”(1994 年)。2000 年，获首届国家最高科学技术奖，奖金额达 500 万元人民币；2006 年，获第三届邵逸夫数学奖，奖金额为 100 万美金。

未来之舟

由于吴文俊的开创性工作，使得中国数学家走在了世界数学机械化发展的前沿。中国政府十分重视该领域的研究。1990 年，中国科学院成立了数学机械化中心。2003 年，该中心又成为数学机械化重点实验室。以吴文俊先生为首的一批国内最杰出的数学家在那里从事研究工作，并且在不断地取得各种成果。

340 年前莱布尼茨的建立“普遍语言符号”体系的理想，至少在数学领域中已有一部分实现。但要完全实现这一理想，可能还需要相当长的时间。

4

数学杰作欣赏

当代数学呈现百花齐放、争奇斗艳的繁荣局面。数学杰作频现，使人目不暇接。前面各章所述，都是富有创意的数学佳作。这里，再叙述一些比较精致的数学作品，让我们共同欣赏。

4.1 RSA 公钥密码术

——互联网通信的安全保障

一把钥匙开一把锁。因此，以往的钥匙是密不示人的。但是，在信息时代，尤其在互联网发达的今天，密码学必须有新的进展，其中的一个特征，就是钥匙必须有公开的一部分。

1. 电子通信安全提上日程

前已提及，德国电气工程师谢尔比乌斯于 1918 年发明了转

轮式“隐谜”机，标志着机械密码时代的到来。波兰和英国数学家则制造出同类结构的“炸弹”机，可以破解“隐谜”。在第二次世界大战期间，这两种机械密码装置之间的较量，曾经在一定程度上改变了战争的进程(详见 3.2 节)。

然而，第二次世界大战结束后，计算机技术开始突飞猛进地发展。在具有超强计算能力的计算机面前，机械式密码显然不堪一击。寻找新的可靠的通信加密方法，成为计算机时代密码专家们所面临的一大难题。

与此同时，电子通信技术也在迅猛发展。继电话和电报之后，又出现了计算机通信网络，它带来了人类信息交换方式的又一场革命，而且影响更深远。1968 年，美国国防部高级研究项目署(Advanced Research Projects Agency，简称 ARPA)正式启动名为“资源共享计算机网络”的建设计划。建成的网络叫做 ARPANET，一开始只连接了美国四所大学。然而 30 年之后，它已发展成为连接到全世界每一角落的 INTERNET——中文名称叫做“互联网”或“因特网”。虽然一开始互联网只是用于军事、科研和教育领域。但人们很早就注意到了它潜在的巨大的商业价值。如果身处异地之人无需直接见面，通过公共的计算机网络就能进行保密通信、交换数据和资料、签署文件和合同，甚至能支付和收取账款，那将是一件多么美妙的事！当然，要实现这一伟大的梦想，首先必须解决一系列有关网络通信安全的问题：其中不仅包括保密通信，还涉及更多的东西。

1976 年，美国斯坦福大学电气工程系的研究员迪菲(Whitfield Diffie，1944—)和教授赫尔曼(Martin Hellman，1945—)联

名发表了划时代的论文“密码学的新方向”:该文不仅澄清了公共计算机网络通信安全的根本问题,而且提出了解决问题的革命性方案。

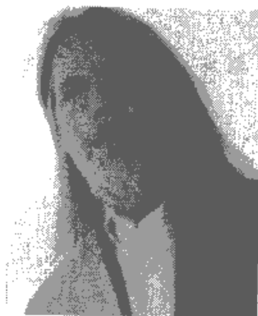


图 4-1　迪菲



图 4-2　赫尔曼

文章指出,计算机通信网络的发展,使得身处世界两端的人们能够很容易地相互联系。但要利用计算机网络做更多的事,首先必须解决两大安全问题:保密和认证。

保密问题很容易理解。为了确保两人之间的网络通信内容不为外人所知,必须对任何一方发出的信息进行加密,对方收到加密信息后再予以解密。但是,无论加密和解密,都需要使用“密钥”。问题的关键是:双方如何传递这个密钥?如果按照传统的密码术,则必须派遣可靠的信使或者双方见面才能传递密钥;那既麻烦又费时,使得网络通信的好处被完全抵消。

认证问题包括身份认证和内容认证。身份认证是要确认网络信息的发送者就是所声称的那个人,既不容旁人冒名顶替,也不容本人事后否认。内容认证是要确认接收者所收到的信息正好是发送者所送出的,既不容外人篡改,也不容接收者或发送者抵赖。这些认证在传统纸质文件中是通过“签名”实现的。因

此，网络通信的认证问题等价于如何实现“数字签名”。

2. 公钥密码系统

可以看到，迪菲和赫尔曼所提出的计算机网络通信安全问题确实与传统密码学所处理的问题大不相同。而且这些问题看上去都很棘手，似乎很难得到解决。然而，他们找到了一个绝妙的解决方案，那就是——“公钥”密码系统。

在“公钥”密码系统中，每位计算机网络的通信者都应该拥有两个密钥，其中一个是对外保密的“私钥”，另一个是对网络上所有人公开的“公钥”。私钥和公钥都可以对信息加密，但私钥加密的信息须用对应的公钥解开，公钥加密则须用对应的私钥解开。

使用公钥密码系统，网络上的任意双方无需事先传递密钥就能进行保密通信。假设在网络上，甲要向乙发保密信息。甲就先用乙的公钥把信息加密，然后发给乙；乙收到信息后，必须用自己的私钥进行解密，才能看到信息的原文（图 4-3）。对于其他任何人来说，由于他们并不掌握乙的私钥，所以不可能看到原文。

使用公钥系统也能够解决认证问题，即实现“数字签名”。

甲要通过网络给任何人发信息时，先用自己的私钥给信息加密，再把它发出。这就相当于甲给所发的信息加上了自己的“数字签名”。因为接收方只有使用甲的公钥进行解密后才能看到信息的原文。这就证明了该信息只能由甲发出，而且其内容

并没有被篡改(图 4-4)。

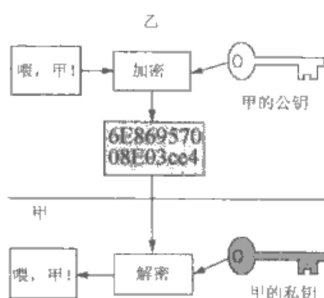


图 4-3

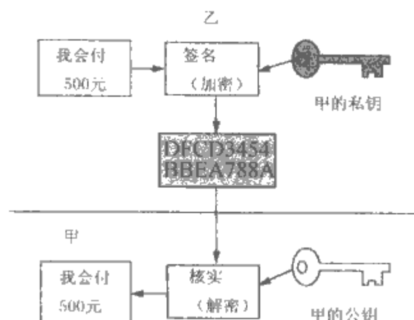


图 4-4

保密通信和数字签名还可以综合起来使用。例如，甲要给乙发信息时，先用自己的私钥对信息加密，再用乙的公钥作第二次加密，然后发出；而乙收到后，必须先用自己的私钥解密，再用甲的公钥作第二次解密，才能看到信息原文。这样就实现了带有"数字签名"的保密通信。

诚如他们的论文题目，迪菲和赫尔曼的工作指明了现代密码学发展的"新方向"。他们所提出的公钥密码系统被认为是密码学思想的一场真正的革命。它不仅可以解决公共网络通信的安全问题，而且将改变密码学仅限于外交、谍报和军事领域中应用的历史，让密码学走向普通民众，走进日常生活。它甚至有可能改变人们的工作和生活方式。

然而，迪菲和赫尔曼并没有说明如何实现公钥密码系统。事实上，当时的人们还不知道是否真能找到具有上述种种功能的"私钥"和"公钥"。不过，事情很快有了圆满的答案。

3. RSA 方法用了古典的数论

1978 年，美国马萨诸塞理工学院计算机科学实验室的三位研究员里维斯特（Ronald L. Rivest，1947—）、沙米尔（Adi Shamir，1952—）和艾德莱曼（Leonard Adleman，1945—），联名发表论文“获得数字签名的方法与公钥密码系统”，文中首次提出了一种实现公钥密码系统的方法。该方法后来就以这三位发明人的首字母命名——被称为“RSA 方法”。

RSA 方法极为巧妙，又非常简单。它基于初等数论中的一条著名定理：

费马小定理　设 p 是任意的大于 2 的素数，a 是任意的与 p 互素的非零整数，则必然有 $a^{p-1}=1 \bmod p$。（其中 mod 表示被除后的余数。）

用 RSA 方法产生私钥和公钥的过程大致如下。

步骤 1　随机地寻找两个大素数 p 和 q（建议十进制数 100 位以上，或二进制数 300 位以上）；计算 $n=pq$，$\varphi(n)=(p-1)(q-1)$。

步骤 2　找一个与 $\varphi(n)$ 互素的合适的正整数 e，则用欧几里得辗转相除法可以找到另一个正整数 d，使得 $ed=1 \bmod \varphi(n)$。

步骤 3　整数对 (e,n) 作为“公钥”放在公共网络上，$(d,\varphi(n))$ 则是“私钥”需要保密。

如果网络用户甲要用 RSA 方法给乙发送一段需要保密的信息 M，根据仙农的数字化信息论，不妨假设 M 是一个正整数

且小于 n ；否则的话，可将 M 分为几段数字，其中每一段都小于 n。于是，甲的加密操作应如下进行。

步骤 1　找到乙的公钥 (e,n)，并计算 $M=M^e \bmod n$ 。

步骤 2　将 M 发送给乙。

乙收到甲发来的 M 后，就用自己的私钥计算 $M \bmod n$。运用费马小定理及其推广可以证明：$M^d=M^{ed}=M \bmod n$。于是，他完成解密得到了信息原文 M。外人并不知道乙的私钥，也无法通过公钥来破解私钥（见以下说明），所以不能获取原文。

通过类似的操作，用 RSA 方法也能够容易地实现数字签名。

RSA 方法之所以可行，是基于以下关于整数运算的若干事实。

（1）可以运用计算机实现两个大整数相乘的快速计算。

事实上，计算两个 m 位数相乘所需要的基本运算次数约为 $m\lg m$。所以，即使是几千位数字的相乘也可以很快完成。

（2）存在寻找大素数的快速计算方法。

数论知识告诉我们，在不大于 n 的正整数中，平均存在着 $n/(\ln n)$ 个素数。因此，对于一个几百位大小的数，在确定了它不含有某个小于 100 的素数因子之后，如果它还通过了费马小定理的检验，那么它极有可能就是素数。运用计算机可以快速完成验证操作。

（3）不存在分解一个大整数的有效方法。

任何人企图破解密文就必须知道私钥(d,$\varphi(n)$)中任意一个值;而想利用公钥(e,n)来算出 d 或 $\varphi(n)$,就必须分解 n。按照当时最快的算法,分解整数 n 约需进行 $n^{\sqrt{\ln\ln(n)/\ln(n)}}$ 次基本运算。也就是说,用当时速度最快的计算机分解一个 50 位的整数需要 3.9 小时,分解 75 位的整数需要 104 天,100 位整数需要 74 年,200 位整数则需要 38 亿年。

事实(1)和(2)保证了我们能够很快地产生足够数量的公钥和私钥以供网络通信使用。事实(3)则确保了 RSA 密码的不可破解。

RSA 令公钥密码系统得以真正实现,使得互联网上的电子商务活动成为可能。1991 年起,互联网逐步向商业领域开放。各种商店和公司开始在网上出现,电子商务活动也随之开展起来。经过 10 多年的快速发展,如今网上购物、网上交易、网上银行、网上财税申报等到处可见,电子钱包、虚拟货币、电子发票和电子合同等数字化凭证也已寻常。

而所有这一切,都依赖于 RSA 公钥密码系统的安全保障。因此,完全可以这样说,正是因为迪菲和赫尔曼创造了公钥密码系统的概念,以及里维斯特等人发明了 RSA 方法,才有了互联网上空前繁荣的今天,才使得互联网能够全面地深入我们的社会,并且改变着我们的学习、工作和生活方式。

2002 年,里维斯特、沙米尔和艾德莱曼"因巧妙地实现了公钥密码系统"而分享了美国计算机协会颁发的图灵奖。

4. 整数因子分解的难度成为关键

由于 RSA 公钥密码术的出现,使得数论领域中原本一个普

通的研究课题——整数分解立即备受瞩目。因为 RSA 方法的安全性完全依赖于“不存在整数分解的有效算法”这一事实，而该事实并未得到理论上的证明。数学家们于是想通过寻找分解大整数的新方法来考验 RSA 密码术。

1977 年 8 月，RSA 方法的三位发明人在《科学美国人》杂志上提出了一段用 129 位整数加密的密文，来向全世界数学家和密码专家挑战。此密文直到 1994 年才被破解。由英美两国数学家联手 600 多位志愿者，利用互联网上1 500台计算机，工作了 8 个月，才算出密文的原文是“THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE”（“神秘之词是易怒的兀鹫”）。他们所使用的整数分解算法叫做“二次筛法”，其要点是设法获得形如 $x^2=1 \bmod n$ 的表达式，这时 $x-1$ 或 $x+1$ 中就可能包含 n 的非平凡因子，从而获得 n 的分解。

目前速度最快的整数分解算法是“数域筛法”（number field sieve，简称 NFS），其数学基础是代数数论。该方法特别适合分解 120 位以上的大整数。1990 年，数学家用 NFS 方法成功地分解了第九个费马数。

数学小知识　17 世纪的法国数学家费马曾经认为，形如 $2^{2^n}+1$的数都是素数。此类数后被称为“费马数”，常记为 F_k。易知 $F_0=3$，$F_1=5$，$F_2=17$，$F_3=257$，$F_4=65\ 537$，它们确实都是素数。但 18 世纪数学家欧拉发现 $F_5=4\ 294\ 967\ 297=641\times 6\ 700\ 417$，不是素数！自那以后，许多费马数被证明不是素数，而且再也没有找到新的素数费马数。

第九个费马数 $F_9=2^{2^9}+1=2^{512}+1$，作为二进制数它有 512

位，其中首尾各为“1”，中间都是“0”；作为十进制数它有155位。著名整数分解专家兰斯特拉兄弟（Hendrik W. Lenstra，1949—；Arjen K. Lenstra，1956—）等从1990年2月中旬开始用NFS方法分解F_9。为了加快进度，他们在互联网上发布通告，要求自愿者贡献多余的机时用于分解计算。结果获得了相当于700多台计算机工作站的无偿帮助。到该年6月中旬终于完成分解，证明了F_9是三个素数的乘积，它们分别是7位数、49位数和99位数。

1999年，F_{10}也被完全分解。虽然是一个多达300多位的大整数，但因为它所包含的一些素数因子不太大，所以最后被成功分解。

鉴于计算机速度的飞快提高和整数分解新方法的不断出现，目前数学家建议RSA公钥密码系统使用250位以上的整数，而且其中所含的素数因子也应在100位以上。这样才能保证整个系统的安全。

未来之舟

受RSA方法的启发，一系列数论和代数学工具开始被用于密码学领域。比如说，利用有限域上椭圆曲线解的Abel群结构性质也能够实现公钥密码系统，而且它比RSA密码系统更有效更可靠。

RSA密码术出现以后，使得整数分解成为热门研究领域，不断地有改进方法或推出新方法。但总的来说，该领域中并没有重大的突破。因此可以说，迄今为止RSA公钥密码系统还是很安全的。不过，因为还没有人能够从理论上证明确实不存在整数分解的有效算法，所以并不能排除突然在某一天，某位数学家找到了快速分解大整数的可行方法。如果这件事真的发生了，谁能想象互联网上将产生怎样的混乱场面！

从计算机发展的角度来看，科学家们正在设想一种全新的计算机——量子计算机。它基于量子力学原理，将比现在的任何计算机快一万倍以

上，而且能够同时处理多种任务。1994 年，在美国电话电报公司贝尔实验室工作的数学家肖尔(Peter W. Shor,1959—)发现在量子计算机上能够实现快速分解整数！肖尔因此于 1998 年获得了由国际数学联盟颁发的奈望林纳应用数学奖。不过，量子计算机的研究至今仍处于理论阶段，人们现在还不知道何时、甚至是否能制造出真正的量子计算机。无论如何，互联网上的密码专家们应做好充分的准备，在真正的量子计算机将要出现之前，必须找到替代 RSA 的新密码技术。

4.2　证明关于斯坦纳树的吉尔伯特-波拉克猜想

美国 AT&T 电话公司，面临一个收费难题。在数学上涉及著名的吉尔伯特-波拉克猜想。中国数学家堵丁柱参与其事。

1. 小题大做

由美国大发明家和企业家、电话发明人贝尔(Alexander Graham Bell,1847—1922)所创建的美国电话电报公司(简称 AT&T)，是一家拥有雄厚财力和强劲科技实力的跨国企业，在国际电子通信技术领域和产品市场中长期占据着统治地位。其属下的贝尔实验室则是一个世界著名的科研机构。世界上第一只晶体管在这里制造；计算机 UNIX 操作系统和 C 程序语言也在这里开发；这里曾经出现了好几位诺贝尔奖获得者；信息论的创立者仙农和控制论创立者维纳也都曾在这里长期工作过。然而，就是这家“科技巨人”的公司，有一次却在电话业务收费问题上，被人捉弄了一把。

美国北卡罗林纳大学的三个分校，恰好位于正三角形的三个顶点(边长假设为 1 单位)。三校打算建设校际间联系的专用

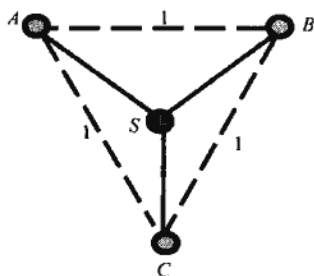


图 4-5

网。按照当时 AT&T 电话公司收费标准，以连接三点的两边长（$=2$）为计费基准。有一天，AT&T 电话公司接到申请，要在北卡三校的中心点（是一处无人居住的沼泽地）装电话。同时，北卡还要求将正三角形的三顶点 A,B,C 以及其中心 S 共四点连接起来（图 4-5）。这样一来，按照 AT&T 公司的收费标准，只需按照 $AS+BS+CS=3\times(\sqrt{3}/3)=\sqrt{3}$（小于 2）为收费基准。

AT&T 公司经过研究，知道北卡大学有能人来给他们出难题了。如果按照现在的规则，在沼泽地安电话、拉线的基础工程都由公司负责，费了好大劲连接了四点，收费却比原来的 2 单位还要少，这岂不是赔本买卖吗？于是，公司向北卡大学提出，沼泽地的电话不要装了，我们就按$\sqrt{3}$收费就是了。事情就这样戏剧性地结束。

从数学的角度看，建造内部电话网络的业务（把这些公司属下处于异地的各个部门用电话线相互连接起来），各个电话公司都是按"最小生成树"原则计算费用。也就是说，根据连接所有相关节点所需最短电话线的长度收费，而不管实际电话线如何连接。

数学小知识　图论是应用数学的一个分支，主要研究由节点（或顶点）和连接这些点的线段所形成图形的种种性质。如果给定图形上任意两个节点总可以通过一些线段连接起来，就称该图是"连通"的；如果给定一个图是"连通"的，而且其中不存在

由一些线段组成的"圈",就称该图是"树"。给定一个节点集 V,其"生成树"是指一个包含且只包含 V 中所有点的"树";V 的"最小生成树"则是指其线段长度之和最小的那个"生成树"。

斯坦纳最小树问题 设在平面上分布有彼此相隔一定距离的 $n(n\geqslant 3)$ 个点,形成点集 V。问如何用一些直线段把 V 中的点连接起来,并使得这些线段的长度之和最小?注意,得到的解必然是一个"树"图形,被称为"斯坦纳最小树";而且其中可能会出现不属于 V 的节点,被称为"斯坦纳点"。

类似于上述北卡大学的例子(图 4-5),含有三个点 A,B,C,这些点彼此距离为 1;它们的"斯坦纳最小树"由 SA,SB,SC 这三个长度相等、夹角均为 120°的线段连接相应点而形成;注意到其中 S 点并不属于 V,因而是"斯坦纳点"。线段 AB,AC 则构成了 V 的"生成树",而且是"最小生成树"。显然在这里,"斯坦纳最小树"的线段之和小于"最小生成树"的线段之和。事实上,

"斯坦纳最小树"的线段之和 $= SA + SB + SC = \sqrt{3}$,

"最小生成树"的线段之和 $= AB + BC = 2$。 (1)

"斯坦纳最小树问题"据说是由瑞士数学家斯坦纳(Jakob Steiner,1796—1863)首先提出的,因此后来以他的姓命名。但历史文献表明,17 世纪法国数学家费马和 19 世纪德国数学家高斯都研究过类似的问题。

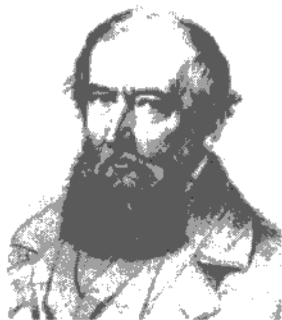


图 4-6 斯坦纳

美国的电话公司后来停止了按"最

小生成树”收费，改为按“斯坦纳最小树”收费。其所属贝尔实验室则开始了对“斯坦纳最小树”的长期研究。人们发现，该问题不仅在建设电话线网络中，而且在设计晶体管集成电路、交通运输和计算生物学等领域中有着广泛的应用。

2. 斯坦纳比率

一般来说，解决斯坦纳最小树问题需要大量的计算。而且随着节点个数 n 的增加，计算量也会很快增长，致使计算机不堪胜任。事实上，已经证明它是个“NP 问题”(参见 5.4 节)，对于此类问题目前尚未找到有效的算法。作为对比，“最小生成树”的计算却很简单。因此在有些场合，还是需要通过计算“最小生成树”来估计“斯坦纳最小树”。

现在的问题是，这两者之间究竟相差多少？人们用它们之间的比值来表示其差别，被称为“斯坦纳比率”。在以上附图的例子中，从式(1)可算出其“斯坦纳比率”为

$$\sqrt{3}/2 \approx 0.866$$

这当然是一个极其特殊的例子，因为所考虑的三个节点正好构成了一个等边三角形。但是在 1968 年，贝尔实验室的两位数学家吉尔伯特与波拉克证明了，当节点个数 $n=3$ 时，总有

$$\text{斯坦纳比率} \geqslant \sqrt{3}/2 \approx 0.866 \tag{2}$$

他们于是猜测不等式(2)对于任意的 $n\geqslant 3$ 都成立。这就是著名的吉尔伯特-波拉克猜想。

自那以后，数学家们一直试图证明这一猜想。其中在贝尔实验室工作的两位台湾资深数学家金芳蓉(1949—)和黄光明

(1940—)曾于1978年合作证明了“斯坦纳比率”$\geqslant 0.742$；1985年，金芳蓉与其丈夫、当时也在贝尔实验室工作的葛立恒(Ron Graham，1935—；著名离散数学家，曾任美国数学会主席)合作，借助于大量的计算机运算，证明了该比率$\geqslant 0.824$。

3. 堵丁柱参与最后证明

终于在吉尔伯特-波拉克猜想提出的第22年，也就是1990年，正在贝尔实验室访问的中国数学家堵丁柱(1948—)与该实验室的台湾籍研究员黄光明合作，证明了这一猜想。即对于任意的节点数$n\geqslant 3$，总有“斯坦纳比率”$\geqslant \frac{\sqrt{3}}{2}\approx 0.866$。

堵和黄采用了完全不同于以往的崭新的证明方法，其要点是把n个节点组成的集合与$2n-3$维空间的点建立起对应关系，使得吉尔伯特-波拉克猜想转化为$2n-3$维空间上的函数极值问题。然后根据极值点的几何性质验证了该猜想的正确性。

堵丁柱和黄光明的成果宣布之后，美国《纽约时报》立刻予以报道。接着，《科学》、《科学新闻》、《SIAM新闻》、《新科学家》等权威刊物也相继转载评述。堵和黄的证明于1992年完整发表，著名的《大英百科全书》随即在其1992年《年鉴》中，把该证明列为当年的数学六大成就之一。

1998年，堵丁柱和黄光明荣获美国运筹研究学会和管理科学研究所联合颁发的CSTS奖。此外，堵丁柱还于1992年获国家杰出青年奖，1996年获国家自然科学二等奖。

堵丁柱是黑龙江省齐齐哈尔市人，从小就喜爱数学。1969年高中毕业后，先后在机车车辆厂和灯泡厂工作。1977年“文

革”结束并恢复高考后，进入中国东北重型机械学院自控系计算机应用(原工业控制系)专业学习，但只就读了几个月就考上了科学院的研究生，导师是著名数学家越民义教授(1921—)。1981年毕业后不久，赴美国求学。1985年获加利福尼亚大学圣·巴巴拉分校的数学博士学位。1987年回国，任中科院应用数学研究所研究员。1991年再赴美国执教。1995年任明尼苏达大学计算机系教授，现任美国得克萨斯大学达拉斯分校计算机科学系教授和中国西安交通大学理学院院长。

未来之舟

关于斯坦纳最小树问题及相应的吉尔伯特-波拉克猜想均可以从平面推广到三维、四维以及更高维空间。当然，高维的情况比平面情况要复杂得多。数学家们已经获得了关于三维及更高维空间斯坦纳问题的一系列研究结果，但要像堵丁柱、黄光明证明平面情况的吉-波猜想那样彻底解决问题，还需走很多路。另外，斯坦纳问题还可以推广到各种非欧几里得距离空间中，这时的情况就更加复杂了。这些推广的斯坦纳最小树问题在多个领域中有广泛的实际应用价值。

4.3 证明关于多体系统非碰撞奇点的班勒卫猜想

根据万有引力定律，我们能够确切地描述太阳、地球、月亮之间的运动关系吗？这个经典问题引出一个非碰撞奇点的猜想。夏志宏作出重要贡献。

1. N体问题和瑞典国王的奖金

在浩瀚的宇宙中，星球的大小可以忽略不计，所以我们可以把它们看成质点。如果不计太阳系其他星球的影响，那么它们

的运动就只是在引力的作用下产生的。所谓 N 体问题是指，在三维空间中给定 N 个质点，如果在它们之间只有万有引力的作用，那么在给定它们的初始位置和速度的条件下，它们会怎样在空间中运动？这三个天体的质量、初始位置和初始速度都是任意的。我们能够据此解出描述它们运动的那些微分方程吗？

在一般三体问题中，每一个天体在其他两个天体的万有引力作用下的运动方程都可以表示成 3 个二阶常微分方程，或 6 个一阶常微分方程。因此，一般三体问题的运动方程为十八阶方程，必须得到 18 个积分才能得到完全解。然而，目前还只能得到三体问题的 10 个积分，还远不能解决三体问题。

1885 年，在刚创刊不久的瑞典数学杂志 *Acta Mathematica* 的第 7 卷上出现了一则引人注意的通告：为了庆祝瑞典和挪威国王奥斯卡二世在 1889 年的六十岁生日，*Acta Mathematica* 将举办一次数学问题比赛，悬赏2 500克朗和一块金牌。而比赛的题目有四个，其中第一个就是找到 N 体问题的所有解。参加比赛的各国数学家必须在 1888 年 6 月 1 日前把他们的参赛论文寄给杂志的创办人和主编 —— 著名的瑞典数学家米塔-列夫勒。所有论文将匿名地被一个国际委员会评判以决出优胜者，然后优胜者的论文将发表在 *Acta Mathematica* 上。这个委员会由三个当时赫赫有名的数学家组成：德国的维尔斯特拉斯(Karl Weierstrass，1815—1897)，法国的埃尔密特(Charles Hermite，1822—1901)和米塔-列夫勒本人组成。

比赛在当时轰动一时。由于问题十分难解，一开始跃跃欲试的数学家后来都知难而退，最后只有四五个数学家真正交了

答卷。所有评委一致认为其中一份答卷对于 N 体问题的解决作出了关键的贡献。这位获胜者就是法国数学家、物理学家庞加莱(Jules Henri Poincaré,1854—1912)。

1885 年的庞加莱只有 31 岁。他的获奖论文“关于三体问题的动态方程”最后于 1890 年在 *Acta Mathematica* 上发表,论文长达 270 页,占了整整半卷杂志。从 1892 年到 1899 年,庞加莱陆续出版了他的三大卷宏伟巨著《天体力学的新方法》。这些工作奠定了现代天体力学、动力系统、微分方程定性理论,甚至混沌理论的基础。这些重要的创见,直到几十年后才被广大的数学工作者所领悟,进而发展成现代的数学理论。

2. 班勒卫猜想

历史上关于 N 体问题中奇点的研究,是和庞加莱同时代的另一位法国数学家班勒卫(Paul Painleve,1863—1933)开始的。班勒卫是巴黎大学数学教授,却从 1914 年到 1933 年去世为止一直在法国政府任内阁部长,并曾两度出任法国总理。1920 年他和另一位著名数学家 E·波莱尔(E. Borel,1871—1956)因考察铁路建设来华访问,顺便在北京、上海作数学演讲。

1895 年奥斯卡二世邀请班勒卫到斯特哥尔摩大学讲学,并亲自到讲演厅和教授、学生们一起聆听班勒卫的精彩演讲。班勒卫在斯特哥尔摩做了 23 次系列演讲,给后人留下了长达五六百页的演讲笔记,而他的主题就是微分方程中超越函数及其对 N 体问题奇点的应用。班勒卫证明了在三体问题,奇点必须是碰撞解,也就是说爆破是不可能在三体问题中出现的。但是在

他笔记的第 588 页，他猜测当 N 大于 3 时，N 体问题存在非碰撞的奇点解。

形象地说，在一只篮球上面放一只网球，然后让它们从你的胸部高度自由下落，你会看到怎样的结果？你会看到网球在篮球的落地反弹作用下，以出人意料的速度飞向空中(图 4-8)。这一奇特现象被称为“弹弓效应”，是由于地球、篮球和网球这 3 个物体，在万有引力的作用下产生连续碰撞而引起的。在这里，通常假设物体运动遵守牛顿定律而不是爱因斯坦相对论定律，即物体的速度不受光速限制而且质量并不随速度改变；另外，为了简化问题，假设物体的体积可以忽略。物体之间的碰撞就发生在奇点时刻。那么，是否存在非碰撞的奇点？这就是著名的“班勒卫猜想”。

1895 年班勒卫证明当 $n=3$ 时，非碰撞奇点不存在；同时他猜测当 $n\geqslant4$ 时，这样的奇点可能存在。在以后的近 100 年里，许多数学家企图证明班勒卫猜想。但在开始时，人们甚至不知道在非碰撞奇点究竟会发生什么事。



图 4-7　班勒卫

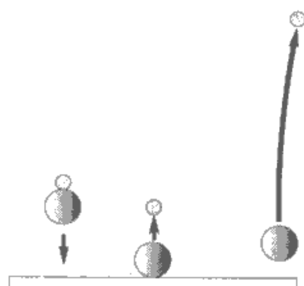


图 4-8

3. 弹弓效应的数学模型

1908 年，瑞典天文学家冯·蔡佩尔（E. Hugo von Zeipel，1873—1959）取得了第一个突破。他证明了一个后来以他的名字命名的定理：

> 如果在一个多体系统中存在非碰撞奇点，则随着时间不断接近该奇点时刻，系统中的物体运动将趋于无界。

也就是说，在奇点附近，物体的运动范围会无限制地扩大。冯·蔡佩尔定理给出了发生非碰撞奇点的一个必要条件。但是，多体系统怎么可能会在有限的时间内发生无限范围的运动呢？由此看来，非碰撞奇点似乎不可能存在。

然而到了 1966 年，美国耶鲁大学的天体力学教授塞拜海伊（Victor Szebehely，1921—1997）和他的学生通过计算机模拟发现，在适当的条件下“三体系统”会产生一种奇特的现象：其中两个物体紧密地互相绕转，另一个物体却以高速飞向远处——这就是“弹弓效应”！

人物介绍 塞拜海伊是著名的“三体问题”专家，匈牙利移民，正是他完成了美国“阿波罗登月计划”中关于“地球—月球—飞船”三体系统的复杂计算，从而保证了人类登月的成功。

这给科学家带来启示：如果能够设法在多体系统中引起一连串“弹弓效应”的振荡，那么物体不就可以通过连续加速而实现有限时间内的无限运动了吗？

果然，在 1975 年，两位美国数学家，普林斯顿大学教授马瑟和明尼苏达大学教授麦吉，成功构造了一个 4 体系统模型：其中 4 个物体都在一条直线上运动，经过连续不断的“弹弓效应”，使得这些物体在有限的时间内飞往无穷。可惜的是，这个系统离不开物体之间的碰撞。因此，“班勒卫猜想”仍然没有被证明。

4. 夏志宏证明班勒卫猜想

1988 年，正在美国西北大学学习的中国青年数学家夏志宏出人意料地在他的博士论文中证明了，当 $n\geqslant5$ 时，非碰撞奇点是存在的！从而除了 $n=4$ 的情况，班勒卫猜想被解决了。

事实上，夏志宏借鉴了马瑟和麦吉的做法，巧妙地构造了一个 5 体系统的模型，其中两对质量相等的物体分别在两个平行平面中围绕一个扁率极大的椭圆运行，而最后一个物体沿着穿过这两个椭圆中心的一条直线上运行(图 4-10)。当该物体刚穿过其中一对物体时，这对物体相互之间距离正好达到极小，从而对该物体形成极大的拉力，使它获得极大的加速度，于是产生了“弹弓效应”；而当该物体穿过另一对物体时，也发生类似的情况；这样该物体在两对物体之间穿梭运行，但不发生碰撞。可以证明在有限的时间内，穿梭物体的速度越来越大直至无限，并且由于它的作用使得两对物体之间的距离也趋于无限——这就产生了非碰撞奇点。

夏志宏 1962 年 9 月 20 日生于江苏省东台市；1982 年毕业于南京大学天文学系，获学士学位；1983 年赴美国西北大学，在著名的动力系统专家萨瑞(Donald G. Saari，1940—)的指导下攻

读博士学位。夏志宏在那里进行着每周 7 天、每天 12 小时以上的勤奋学习和研究，终于取得了解决“班勒卫猜想”的重大突破。当他把这一成果写成近百页论文投寄美国著名的数学期刊《数学纪事》(*Annals of Mathematics*)后，审稿专家无法断定其中的证明是否正确。期刊编辑部直到两年后才给了作者一个含糊的回答，指出证明中有些地方难以令人信服，要求进行修改。夏志宏把修改后的论文重新寄出。这次审稿者就是那位著名的“班勒卫猜想”研究专家马瑟，他在所执教的普林斯顿大学组织了一个讨论班来讨论夏的论文。经过 1991 年秋季整整一个学期的讨论，最后的结论是：夏志宏的证明是正确的。于是，论文终于在 1992 年正式发表。它标志着已有近百年历史的“班勒卫猜想”终于被基本解决(除了 $n=4$ 的情况)。



图 4-9　夏志宏

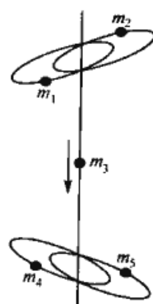


图 4-10

夏志宏由于这一杰出的工作，于 1993 年获得了美国国家科学基金会的青年研究者奖和美国数学会的首届布卢门塔尔奖。

夏志宏还用变分方法研究动力系统中的“阿诺尔德扩散”取得一系列成就，其中一个成果是把庞加莱关于带有一个无限小质量物体的“三体问题”的结果推广到了全部是有限正质量物体

的情况。他为此于 1996 年获得美国马里兰大学的马丁奖，并获得在 1998 年国际数学家大会上作 45 分钟报告的殊荣。

夏志宏于 1988—1990 年任哈佛大学助教授，1990—1994 年任乔治亚理工学院副教授，1994 年起回到西北大学任数学教授。1998 年入选中国教育部第一批“长江计划学者”名单，兼北京大学特聘教授。

未来之舟

班勒卫猜想还剩下 $n=4$ 的情况尚未解决。虽然种种迹象表明，在 4 体系统中不太可能有非碰撞奇点存在；但迄今为止还没有人能够从数学上严格证明这一点。

动力系统是现代数学中一个极其活跃的分支，起源于多体问题研究的这门学科无论在理论上还是在应用上都具有非常重要的意义。除了“奇点”之外，动力系统的另一个研究热点是“混沌”：它是指非线性动力系统中不可预测、不可重复、貌似随机的物体运动。科学家们惊讶地发现，“混沌”在自然界和日常生活中到处可见，是非线性确定系统的一种固有特性。“混沌学”已经成为又一门新兴科学研究分支。

4.4　数学奇葩

——分形几何

在各种出版物的封面和插页里，都可以看到用计算机构造出来的美丽图形：分形。经过 30 多年的努力，今天的分形既是一门严肃的数学分支，成为数学家的研究对象；又是一门艺术，赢得无数艺术家的青睐。此外它还是图像压缩、信息传输的工具，以至可以成为一种上帝创造的指纹，在鉴定特定的地质纪元、矿脉类型及其含量的研究中发挥作用。

1. 分形是一种几何

我们熟知的几何是欧几里得几何，有较高数学修养的还知道黎曼几何、非欧几何等等。在这些几何空间中可以引进坐标架，建立坐标，也可以引进维数的概念。一个物体的欧氏维数是能容下它的空间之最低维数，而拓扑维数则是其独立坐标的个数。

欧几里得几何、黎曼几何、非欧几何等研究的对象是直线、圆、平面、球、锥面等等，这些都是从客观世界中抽象出来的几何对象。因此也可以说欧几里得几何、黎曼几何、非欧几何等是理想化了的几何。

然而，我们日常见到的图形并不都是理想化的图形。一座大山，像锥又不是锥；一棵大树，像球又不是球；海岸线、河岸线，像折线又不是折线。

1973 年，曼德勃罗(B. B. Mandelbrot，1924—)在法兰西学院讲课时，首次提出了分形和分形几何的设想。分形(Fractal)一词，是曼德勃罗创造出来的，原意指那些具有不规则、支离破碎等意义上的图形。事实上，弯弯曲曲的海岸线，起伏不平的山脉，粗糙不堪的断面，变幻无常的浮云，九曲回肠的河流，纵横交错的血管，令人眼花缭乱的满天繁星等，共同的特点是，表面上极不规则或极不光滑，内涵中却具有某种特定的结构。研究物体的分形结构的几何学称为分形几何。

分形几何与传统几何相比有两个特点。首先从整体上看，分形几何图形是处处不规则的。例如，海岸线和山川形状，从远

距离观察，其形状是极不规则的。其次，在不同尺度的局部上看，图形的规则性又是相同的。上述的海岸线和山川形状，从近距离观察，其局部形状又和整体形态相似，它们从整体到局部，都是自相似的（除了一些用来描述混沌和非线性系统的分形，并不完全自相似）。

2. 分形的例子

（1）Cantor 集

在许多数学书中提及的 Cantor 集，就是一个一维分形。它的构造过程为：将区间[0,1]三等分，去掉中间的一段，将左右两段分别再三等分，各去掉中间一小段，如此重复，余下部分的极限即为 Cantor 集，如图 4-11 所示。

（2）科赫雪花

将一条线段分为三段，以中间一段为一边向外作一等边三角形，然后将这一段去掉，加上等边三角形的余下两边，对所得长度为原来 1 /3 的四条小线段重复上述操作，即得科赫雪花，如图 4-12 所示。

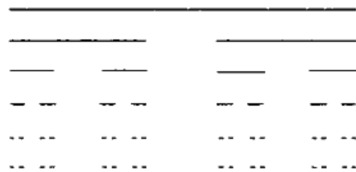


图 4-11　Cantor 集的构造过程



4-12　科赫雪花曲线的构造过程

（3）Sierpinski 地毯和 Sierpinski 海绵

将一个正方形等分成 9 个小正方形，去掉中间一个，对其余

8 个重复上述过程，即得 Sierpinski 地毯，如图 4-13 所示。

将一个正方体等分成 27 个小正方体，将不在大正方体棱边上的 7 个去掉，对余下的 20 个重复上述过程，即得 Sierpinski 海绵，如图 4-14 所示。

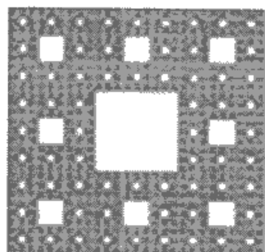


图 4-13　Sierpinski 地毯

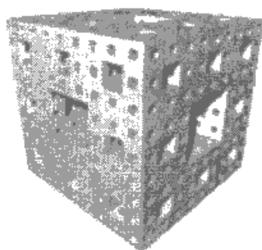


图 4-14　Sierpinski 海绵

3. 分形的维数

让我们先来看看几何对象的维数是如何定义的。

维数与测量有密切关系，测量一个几何图形时要用一个与图形的维数 d 相一致的“单位”l^n（$n=d$ ）去测，才会有确定的结果。例如，量体积要用立方体 l^3 为单位，量面积要用正方形 l^2 为单位，量长度要用线段 l 为单位，等等。如果“单位”的维数 n 与几何图形的维数 d 不相等的话，那么 $n<d$ 时结果为无穷大；$n>d$时结果为零。也就是说，当$n\neq d$时，这个“单位”不能用来测量几何图形。

事实上，几何与尺度是密切相关的。首先让我们来观察长度和维数与尺度的关系。

如果让两个小组来度量长江的长度，其中一组以 10 米为单位，而另一组以 1 厘米为单位。最后我们发现，两个小组量得的

长度有很大的差别，后一组所量得的长度要比前一组量得的大得多。这是因为河岸线、海岸线都具有分形结构，当度量单位趋于零时其长度趋于无穷大。

让我们再来考察一个毛线球的维数。我们先在 200 米的距离上来观看它，这时它是一个点，是零维的。其次在 20 米的距离上来观看它，这时它是一个球，是三维的。再在 2 米的距离上来观看它，这时它是由毛线绕成的一个球，是 1 维的。最后在 2 厘米的距离上来观看它，这时可发现绕成球的毛线是由千丝万缕的绒毛按相似的结构织成的。

分形维数的定义有很多种，如：Hausdorff 维数、自相似维、容量维、信息维、关联维、Lyapunov 维、盒子维等等。下面我们给出自相似维和盒子维的定义。

定义 4.1　若 $A \subset \mathbf{R}^n$ 总可以逐级分成 N 个同样大小的与原集合相似的子集，每次的缩小因子为 $\frac{1}{b}$，则称

$$D_s = \frac{\ln N}{\ln b}$$

为 A 的自相似维数。

例　Koch 曲线的自相似维数为 $D_s = \frac{\ln 4}{\ln 3} = 1.2619$，Sierpinski 三角形的自相似维数为 $D_s = \frac{\ln 3}{\ln 2} = 1.585$。

定义 4.2　设 $A \subset \mathbf{R}^n$，用边长为 $\frac{1}{2^n}$ 的小盒子去覆盖 A，$N_n(A)$ 表示盖满 A 所需的最少盒子数，则称

$$D=\lim_{n\to\infty}\frac{\ln N_n(A)}{\ln 2^n}$$

为 A 的盒子维。

盒子维是目前应用最广泛的一种维数，这主要是因为它非常容易由计算机求得。若将边长为 $\frac{1}{2^n}$ 的小盒子改为半径为 ϵ 的小球，则得到容量维。

4. 走近曼德勃罗

分形理论创始人是美籍法国数学家B·B·曼德勃罗。他1924年11月20日生于波兰华沙一个立陶宛犹太人之家。其父是一位成衣批发商，母亲是位牙科医生。1936年全家移居法国巴黎。他的叔叔索列姆·曼德勃罗(Szolem Mandelbrot，1899—1983)，是一位杰出的纯数学家和复分析专家。在叔叔的影响下，B·B·曼德勃罗于1947年毕业于著名的巴黎多科理工学校。然后去美国，于1948年即获美国加利福尼亚理工学院硕士学位。1952年获巴黎大学哲学(数学)博士学位。1958年定居美国，曾在哈佛大学教经济，耶鲁大学教工程，爱因斯坦医学院教生理学。现为美国IBM公司沃特森研究中心自然科学部高级研究员，哈佛大学应用数学兼职教授，美国国家科学院院士，美国艺术与科学研究院成员，欧洲艺术、科学和人文研究院院士(巴黎)。1980年代以来，获得了许多荣誉。1985年获巴纳德奖章，此奖是由美国国家科学院和哥伦比亚大学颁发的科学功勋服务奖，授予在“物理或天文学方面作出重大发现”或“使科学造福于人类取得新成就”的优秀人物。1986年获富兰克林奖章。

1988年共获四项大奖，其中“科学为艺术”奖的目的是“促进艺术、科学和工业界之间的相互渗透的重大科学创新，从而使美学创造力伸展到科学技术领域中”。1989年获得在以色列海法颁发的“科学与艺术哈维奖”。

曼德勃罗的经历也是不平凡的。由于战乱，他的学业时断时续，受的教育也很不正规。他声称自己从未认真学习过字母，也没有系统地背诵过乘法口诀，只背过五以下的乘法表。年轻时参加过法国著名的数学团体即布尔巴基学派，但由于布尔巴基学派崇尚抽象，摒弃一切直观图像，使得他无法忍受过度的形式主义禁锢，最后而成了一位叛逆者。

他长期生活在一个不时髦的数学角落里，用一种非正统的方法探索一些“不受欢迎”的原理。对纯粹的数学家来说，曼德勃罗并非数学家，他经常受到指责和批评。他曾在世界名人录自己的条文下写道：“如果(与体育一样)把竞技放在一切之上，科学便被污染了。如果为了讲清竞赛规则而使自己退于狭窄的专门技巧之中，科学就要毁灭。有少数学者，他们是一切定型的学科之间的选择性游牧民，他们对于定性学科的智力福利事业大有好处。”

为了给自己的研究对象，即那些极不规则、破碎不堪、不光滑、不可微的东西命名，1975年冬创造了fractal一词之后，著作《分形：形状、机遇和维数》法文版于同年出版。这是一本漫谈式的书，插图丰富，才思横溢，博学而古怪，引起许多议论。1982年经扩展和加工的另一本书，英文版的《大自然的分形几何学》又与读者见面。此书文字艰涩，幽默转折，引经据典，旁征博引，他

自称既是一本"宣言书"又是一本"个案记录",但被分形界的学者视为"圣经"。

5. 动力系统中的分形集

从海岸线有多长那样的问题出发,按照自相似性的观点,研究了科赫曲线、Sierpinski 地毯和 Sierpinski 海绵那样的分形结构,这只是分形几何的第一步。分形和动力系统结缘,使得分形成为非线性数学的一部分,进一步体现了分形更重要的数学价值。

动力系统的奇异吸引子通常都是分形集,它们产生于非线性函数的迭代和非线性微分方程中。1963 年,气象学家洛伦兹(E. N. Lorenz,1917—2008)在研究流体的对流运动时,发现了第一个奇异吸引子,并以他的名字命名,它是一个典型的分形集。1976 年,法国天文学家伊侬考虑标准二次映射迭代系统时获得的伊侬吸引子,也具有某种自相似性和分形性质。1986 年,劳威尔将斯梅尔的马蹄映射变形成劳威尔映射,其迭代下不稳定流形的极限集成为典型的奇异吸引子,它与水平线的截面为康托集。1985 年,格雷波基等构造了一个二维迭代函数系统,其吸附界是维尔斯特拉斯函数,并得到盒维数。1985 年,迈克多纳和格雷波基等得到分形吸附界的三种类型:(1)局部不连通的分形集;(2)局部连通的分形拟圆周;(3)既不局部连通又不是拟圆周。前两者具有拟自相似性。

动力系统中另一类分形集来源于复平面上解析映射的迭代。法都(P. I. J. Fatou,1878—1929)和裘立雅(G. M. Julia,

1893—1978）早在 1918—1919 年开创这一研究。他们发现，解析映射的迭代把复平面划分成两部分，一部分为法图集，另一部分为裘立雅集(J 集)。他们在没有电子计算机帮助的情况下，凭深邃的洞察力，察觉出许多迭代复数列的行为。随后的 50 年，这方面的研究没有得到什么进展。随着电子计算机的出现，这一研究课题重获生机。1980 年，曼德勃罗用计算机绘出用他名字命名的曼德勃罗集(M 集)的第一张图来。

6. 曼德勃罗集与裘立雅集

我们来考察由极其简单的迭代法则生成的具有意想不到的复杂结构的分形图。考虑复函数(复映射)，曼德勃罗集可以用复二次多项式

$$f_c(z) = z^2 + c$$

来构造 。其中 c 是一个复参数。对于每一个 c，从 $z=0$ 开始用 $f_c(z)$进行迭代。我们得到一个复数数列 $(0, f_c(0), f_c(f_c(0)), f_c(f_c(f_c(0))), \cdots)$。这个数列或者发散到无限大，或者是有界的数列。所谓曼德勃罗集合，就是使以上序列为有界数列的那些复数 c 所成的集合。这些 c 点的集合在图 4-15 中就是黑色的部分。

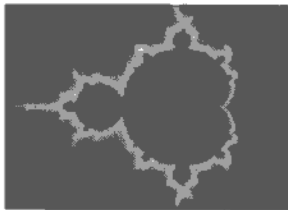


图 4-15　曼德勃罗集

值得我们注意的是，这个集合的边缘，有非常美丽的自相似性。无穷的魅力使得人们将曼德勃罗集称为数学恐龙。

现在我们从另外的角度考虑迭代。这时，让常数 c 固定，而

迭代的初始值 z_{-0} 不再是 0，而可以是任意复数。这时，由初始值 z_{-0} 迭代之后形成的复数列，如果是稳定的，即正则收敛，那么说 z_{-0} 属于法都集；否则，即由 z_{-0} 生成的数列是混沌的，就说 z_{-0} 属于裘立雅集。这样，对于上述的二次迭代来说，当 c 给定之后，就把复平面分成两部分：法都集和裘立雅集。

现在，再来谈曼德勃罗集与裘立雅集之间的关系。如果常数 c 取自曼德勃罗集，那么与 c 相应的裘立雅集是连通的。反之亦然。

因此，它们之间的关系可以比作书和页，曼德勃罗集是一本巨大的书，而一个裘立雅集只是其中的一页。根据点 c 是否在曼德勃罗集之内部，就能够预测相应的裘立雅集的外形及大小。曼德勃罗集是一本可以查阅所有裘立雅集的词典。裘立雅集有自相似性质，而曼德勃罗集没有这种性质。

常数 $c=1-a$ 时，二次迭代产生裘立雅集，a 是黄金比。$c=-0.123+0.745i$ 时，生成的裘立雅集称为 Douady 的兔子分形（图 4-17）。

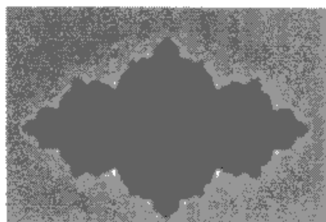


图 4-16

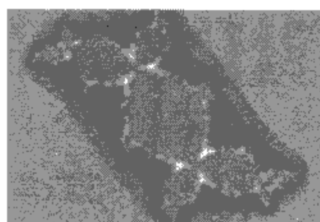


图 4-17

未来之舟

复平面上使裘立雅集 $J(f_c)$ 成为连通集的点 C 组成 M 集，即曼德勃罗集。尤更斯和培特根认为，M 集的性质过去一直是并且将来继续是数学研

究的一个巨大难题。通过将数学理论与计算机图形学实验加以融合，及道迪、息巴德等人在这方面进行的基础性研究工作，在解决这一难题方面已取得重大进展，使人们加深了对 M 集的了解。道迪和息巴德 1982 年证明 M 集是连通的和单连通的，人们猜测 M 集是局部连通的，目前每一张计算机图形都证实了这一猜测，但至今还没有人能给予证明。M 是否为弧连通，目前尚不清楚。M 集边界的维数也是值得研究的问题之一。

"病态"的几何结构原本是极其自然的，自然界的许多东西的几何图形可以由极其简单的演化规则演化而成。分形理论有助于解释为什么少量的遗传物质(遗传密码)可以发育成极其复杂的结构，正如一条 Peano 曲线可以"填满"一个正方形、占人体 5% 的血管布满了人体的每一部分一样。作为一门有着广泛应用的数学分支，分形已经进入各门科学，进入学生的课堂，进入寻常百姓的日常生活，甚至已被制成引人入胜、启迪智慧、老少皆宜、百看不厌的"连环画"。

4.5　攻克斯坦纳三元系大集的百年难题

组合数学是一门古老的学问。主要研究离散对象(通常是有限个)按一定的规则进行组合或排列的问题。近代的组合数学有许多有趣的问题。从柯克曼女生问题到三元系大集问题，这个困扰数学家多年的难题，由中国包头第九中学的一个物理教师所解决。他在特别困苦的研究环境中呈现的精神，使人肃然起敬。

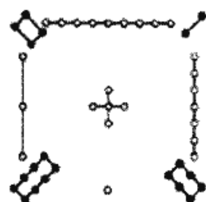
1. 从河图洛书说起

这门数学分支几乎与几何和代数一样古老。如在中国，传说 4 000 年前大禹治水时所发现的"洛书"，其实就是一种奇妙的数字排列图(图 4-18)。在该图中，1 至 9 这九个数字均正好出现

一次，使其按各行、各列、斜线相加的数字之和正好等于 15。用组合数学的语言：洛书是一个三阶纵横图，也称为三阶幻方。宋朝数学家杨辉在他的《续古摘奇算法》(1275 年)中给出了从三阶到十阶的纵横图。

组合数学另一个较古老的研究对象是拉丁方。这是把每种有 n 个的 n 种元素放在一个 $n\times n$ 的方格图中，使得每种元素在每行每列中正好出现一次。如图 4-19 所示就是一个 4×4 的拉丁方。

随着科学技术的迅速发展，特别是计算机的出现，使得组合数学在物理学、化学、生物学、信息科学、生产管理等领域找到了广泛的应用。比如说，拉丁方在实验设计的概率统计理论中就有重要的应用。



4	9	2
3	5	7
8	1	6

图 4-18　中国古代的“洛书”及其对应的数字表示图

A	B	D	C
B	C	A	D
C	D	B	A
D	A	C	B

图 4-19

组合数学的研究主要使用归纳法和递归运算法等方法，并不需要太多的分析、微分几何和抽象代数等现代数学核心工具。这些工具一般只适用于处理连续对象而不太适用于离散对象。因此，组合数学的入门较容易。然而在这门学科中，存在着许多足以难倒最富有才智数学家的有趣的难题。如与“柯克曼女生问题”密切相关的斯坦纳三元系其实是拉丁方概念的一种推广，其中就含有一些曾经长期未能解决的问题。

2."柯克曼女生问题"引出斯坦纳三元系和柯克曼三元系

曾主持筹建华东师范大学数学系和江西大学数学系的中国数学家孙泽瀛(1911—1981),在 20 世纪 50 年代初写过一部甚有影响的数学科普著作《数学方法趣引》(1953 年),其中介绍了哥尼斯堡七桥、哈密顿周游世界、四色地图、幻方等八个有名的数学问题,而他最后介绍的就是"柯克曼女生问题"。书中写道

> 某地一个学校内,有收容 15 个女生的宿舍一所。为了健康的目的,三人一组地分为五组,作郊外散步的计划。如果每组的人,每天全是同样的人,当然感觉到乏味,而且同学之间的友谊,也不能发展。因此规定在每一周,任何人都有与其他同学一度同组之机会。究竟应当怎样分配学生,才合乎这个理想?这实在是一个使舍监煞费思考的问题。也就是所谓的柯克曼女生问题。

这一问题是英国数学家柯克曼(Thomas Penyngton Kirkman,1806—1895)在 1850 年提出的。用数学语言把该问题抽象化,就有如下的叙述。

给定一个含有 $v=15$ 个元素的集合 S,要求设计一个由 S 的若干个 $k=3$ 元子集(称为"区组")构成的子集族 B,使其满足:

(1)S 的每个元素恰在 $r=7$ 个区组中;

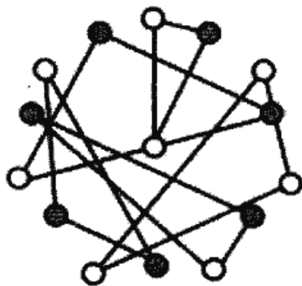


图 4-20

(2)S 的每个二元子集恰在 $\lambda=1$ 个区组中；

(3)B 中所有的区组恰可以形成 S 的 $b=7$ 个划分。

满足以上条件(1)和(2)的组合设计，被称为“斯坦纳三元系”，记为 $B[3;1;15]$。一般地可以有 $B[k;\lambda;v]$，称为“斯坦纳系”，其正式名称叫做“平衡不完全区组设计”。注意，条件(1)中的 $r=7$ 可由参数 k,λ,v 推出。斯坦纳(Jakob Steiner，1796—1863)是瑞士数学家，4.2 节中曾提到另一个以他的姓命名的数学概念——斯坦纳树。如果不仅满足条件(1)和(2)，还满足条件(3)，该组合设计就被称为“柯克曼三元系”，记为 $RB[3;1;15]$。一般地可以有 $RB[k;\lambda;v]$，称为“柯克曼系”，其正式名称叫做“可解平衡不完全区组设计”。注意，条件(3)中的 $b=7$ 也可由参数 k,λ,v 推出。

研究斯坦纳三元系和柯克曼三元系的主要任务，是要确定使 $B[3;1;15]$和 $RB[3;1;15]$存在的所有的 v，并要了解那些存在解的种种性质。“柯克曼女生问题”就是 $RB[3;1;15]$，已经知道它的解是存在的。孙泽瀛在书中给出了两组答案：

用 0—14 编号来表示 15 位女生。

答案一

周日 0 1 4;2 13 14;3 5 11;6 7 10;8 9 12

周一 0 2 8;1 7 14;3 10 12;4 11 13;5 6 9

周二 0 3 14;1 8 10;2 9 11;4 6 12;5 7 13

周三 0 7 9;1 12 13;2 6 3;4 5 8;10 11 14

周四 0 5 10;1 6 11;2 7 12;3 8 13;4 9 14

周五 0 6 13;1 3 9;2 4 10;5 12 14;7 8 11

周六 0 11 12;1 2 5;3 4 7;6 8 14;9 10 13

答案二

周日 0 1 4;2 9 11;3 10 12;5 7 13;6 8 14

周一 0 2 8;1 12 13;3 4 7;5 6 9;10 11 14

周二 0 3 14;1 2 5;4 6 12;7 8 11;9 10 13

周三 0 5 10;1 6 11;2 7 12;3 8 13;4 9 14

周四 0 6 13;1 7 14;2 4 10;3 5 11;8 9 12

周五 0 7 9;1 8 10;2 3 6;4 11 13;5 12 14

周六 0 11 12;2 13 14;4 5 8;1 3 9;6 7 10

斯坦纳三元系存在的充要条件已经得到,那就是

$$v>1 \text{ 且 } v=1,\ 3\bmod 6。$$

但是柯克曼三元系存在的充要条件当时尚未完全确定。孙泽瀛最后指出:如何由斯坦纳系划分为几个柯克曼系,这又是一个很难解决的问题,至今尚未有肯定的答案。

3. 陆家羲的功绩

孙泽瀛可能从未想到,他写的《数学方法趣引》这本薄薄的书,会让一位普通的中国青年跳入深深的数学之河。在以后的 20 多年里,这位青年在艰苦的环境中孤军奋战,竟然独立解决了一连串斯坦纳系和柯克曼系的难题,震动了中外数学界。这位令人肃然起敬的中国数学家就是陆家羲。



图 4-21　陆家羲

陆家羲 1935 年 6 月 10 日出生于上海一个贫苦的市民家

庭。父亲以贩卖酱油精为生，以微薄的收入供儿子读书。14 岁读初中时，父亲不幸病逝，他只好辍学，到一个汽车五金行做学徒工。1951 年考入东北电器工业管理局统计训练班，3 个月后分配到哈尔滨电机厂生产科任统计。业余时间补习高中课程。

1957 年，陆家羲考入东北师范大学物理系。就在这一年，他看到了《数学方法趣引》这本书，被其中的“柯克曼女生问题”深深吸引，竟开始下决心要研究它。

1961 年大学毕业后，陆家羲先后在内蒙古包头钢铁学院、包头市教育局教研室工作，接着又到包头几个中学任教，最后留在包头九中任物理老师。在以优异的成绩完成本职工作之余，他花费了大量的时间、精力和金钱来从事自己的研究。他利用假期坐火车去北京，在北京图书馆查阅最新的中外组合数学专著和期刊。为了节省钱，甚至晚上就和衣睡在北京火车站的广场上。

就在 1961 年，陆家羲证明了 $RB[3;1;v]$（柯克曼三元系）存在的充要条件是 $v\equiv3 \bmod 6$；并证明了 $RB[4;1;v]$（柯克曼四元系）存在的充要条件是 $v\equiv4 \bmod 6$。他把写好的论文几度投给了国内的一些数学期刊。遗憾的是，当时国内并没有多少人了解组合数学。他的投稿均遭退回。（可惜审稿人中没有孙泽瀛，否则情况可能会完全不同。）

10 年以后，1972 年，柯克曼三元系和四元系存在的充要条件先后被外国数学家证明。陆家羲失去了本应属于他的荣誉。

1979 年，陆家羲又证明了一般柯克曼系 $RB[k;\lambda;v]$ 存在的充要条件是

$$v \equiv 0 \bmod k，且\ \lambda(v-1) \equiv 0 \bmod (k-1)。$$

这一结果终于被发表在1984年第4期的《数学学报》上。仅凭此项成果就足以使他跻身一流组合数学家之中。但是，陆家羲很快取得了另一项真正令国际组合数学界感到震惊的成就：他解决了一个已有130年历史的关于斯坦纳三元系的区组设计难题！

如前所述，如果一个斯坦纳三元系 $B[3;1;v]$ 存在解，那它可能有好几个解，即存在不同的区组族，它们都满足给定的条件。这时，如果这些区组族彼此之间不存在共同的区组，就称它们是不相交的。简单的计算告诉我们，$B[3;1;v]$ 最多只可能有 $v-2$ 个不相交的区组族。如果它们真的达到了 $v-2$ 个，就称这些区组族是 $B[3;1;v]$ 的大集。由此产生了组合数学中的一个著名的问题：对于怎样的 v，$B[3;1;v]$ 的大集才能存在？该问题早在19世纪50年代就已提出，但直到1980年这130年里，人们只得到了零星的结果。

1983—1984年，国际著名的《组合论杂志》(*Journal of Combinatorics Theory*)罕见地在两期中连续发表了陆家羲的6篇论文。这6篇论文的总题目是"论不相交斯坦纳三元系的大集"，其中证明了这样的一个定理：

如果

$$v \equiv 1,3 \bmod 6，v>7\ 且\ v \notin \{141,283,501,789,1\,501,2\,365\}，$$

那么斯坦纳三元系 $B[3;1;v]$ 的大集就存在。

陆家羲在论文中巧妙地建立了一些基于素数因子的递归关系，并精心设计了一个等价的正交拉丁方系，最后终于基本解决

了这个已有 130 年历史的斯坦纳三元系大集问题。

4. 新星陨落

一名普通的中学物理教师竟然解决了组合数学中的百年难题，陆家羲在中国数学界引起了轰动。于是，人们开始破格邀请他参加各种学术会议，并请他作大会报告；国内几所大学也打算要聘任他。一切已开始变得美好，他终于有可能在一个良好的环境中自由地从事真正喜爱的研究工作，从而能够取得更多更好的学术成就。然而就在这时，不幸的事发生了。1983 年 10 月 31 日，他从武汉开会结束，途经北京，连夜搭硬座车回包头，积劳成疾的陆家羲因突发心脏病去世。就像一颗新星，突然在夜空闪耀之后，又遽然而逝，令人不胜惋惜。他付出的太多，而我们给予他的支持太少了。

两个月后《人民日报》和《光明日报》等大报，都在显著位置报道了陆家羲的事迹。全国人民都知道了这位不平凡的中学物理教师。

1987 年，陆家羲因“关于不相交斯坦纳三元系大集的研究”而荣获国家自然科学奖一等奖。这是国内数学家所能获得的最高奖励。在此之前，只有华罗庚、吴文俊和陈景润等获得过该奖。

未来之舟

陆家羲的关于“不相交斯坦纳三元系的大集”的存在性证明中，还遗留下 6 个例外值没有解决，即当 $v\in\{141,283,501,789,1\ 501,2\ 365\}$ 的时候。他已经拟就了解决这些例外值的大纲，可惜没有来得及实施。1989 年，美国数学家泰林克证明这 6 个值上的斯坦纳三元系的大集也存在。至此，

“不相交斯坦纳三元系的大集”存在性的充要条件已被完全确定。

然而，关于“不相交柯克曼三元系的大集”存在性的问题迄今尚未被解决。也就是说，孙泽瀛在其“柯克曼女生问题”中最后提出的那个问题，目前还没有找到答案。由于陆家羲工作的影响，组合数学的研究在中国开始蓬勃发展，并且不断取得一流的成果。南开大学于 1997 年成立了组合数学中心，并创办了有国际影响的英文刊物《组合年刊》(*Annals of Combinatorics*)。2008 年 7 月 20—23 日在华东师范大学召开了“第三届全国组合数学与图论大会”，参会代表多达 500 余名，并且有 160 多个大大小小的会议学术报告。该大会见证了我国组合数学研究事业的兴旺和发达。

5

数学无国界

第一次国际化的数学家大会，在 1897 年举行。这是国际数学联盟(International Mathematical Union，IMU)的开端。为了纪念 IMU 开展活动 100 周年，曾任 IMU 秘书长的莱赫托(Olli Lehto，1925—)，受执委会的委托，编写了一部有关“国际数学联盟”的历史。书名是《数学无国界》(*Mathematics Without Border*)。确实，今天的国际数学界，克服了许多政治上的阻碍和困难，努力保持着数学家的团结。这一章，我们将看到 IMU 的各种活动，包括菲尔兹奖的颁发。最后，介绍一个新世纪面临的重大数学问题的清单，其中每个悬赏百万美元。

5.1 国际数学联盟简史

国际数学联盟是当今最广泛、最具权威的国际性数学组织。“数学无国界”是它的宗旨之一。1986 年，中国数学会和位于台

北的数学会，作为一个整体加入国际数学联盟。2002 年，北京举办“国际数学家大会”。

1.19 世纪末的国际数学活动

国际数学联盟在第一次世界大战之后的 1920 年方始成立。不过在它之前，有组织的国际数学合作早已存在。具有明确章程和目标的国际数学家大会从 1897 年起开始定期举行。

19 世纪后期，数学研究继续加速发展。与此同时，已成立的一些全国性的数学团体在积极活动，数学家们在国家的层次上进行联系，以期推动国际范围内的数学合作。

创立集合论的乔治·康托早已感觉到需要在文献书目领域以外开展有组织的国际数学合作。他是德国哈雷大学的教授。1888 年曾提出在政治上互相对立的德国和法国数学家应在一个中立地区会面。1894 年康托在写给俄罗斯数学家 A·瓦西里耶夫的信中提到，他心中酝酿国际大会的想法已有五年。同康托一样，克莱因也认识到了国际合作对于数学的重要性。在 1893 年于芝加哥举行的一次大会的开幕式上，克莱因作了题为“数学的现状”的发言，发言的结尾部分可以浓缩成这样的口号：“全世界数学家，联合起来！”

1894 年，在杂志《数学家中》(*L'Intermédiaire des Mathématiciens*)第一卷的前言中，编辑 Laisant 和 Lemoine 表达了与克莱因在芝加哥所表达的十分类似的想法。他们敦促组织国际数学家大会。

1896 年，瑞士数学家们正式同意举办第一届国际数学家大

会，它将在苏黎世的联邦综合科技学校（现在改名为联邦高等工业大学）举行，时间是 1897 年 8 月 9—11 日。以现代的标准衡量，苏黎世大会时代的数学社会的规模还是很小的。但仍然有来自 16 个国家 208 位数学家参加了大会。中欧的代表占了绝大多数，美国来了 7 人，英国只来了 3 位数学家，出席人数如此之少可能是由于英国的某种孤立主义倾向。

第二届国际数学家大会于 1900 年 8 月 6 日至 12 日在巴黎举行，H·庞加莱任大会主席。C·埃尔米特当选名誉主席。该大会是当年召开的约 200 个科学会议中的一个，它们都是世界博览会的一部分。与其他的大多数会议不同，国际数学家大会已经具有常设性。有 253 位数学家参加，比三年前参加苏黎世大会的人数增加了 20%。在数学史上它因为希尔伯特的演讲而被记住，希尔伯特在他的演讲中预言了 20 世纪的数学发展，并提出了他的著名的 23 个问题。在演讲的结尾部分，希尔伯特表达了与克莱因在 1893 年所表达的极为相近的观点，他这样说："我们不得不面临这样的问题：数学是否也将经受其他科学早已经受的历程，即被分化成一些分支学科，这些学科的专家们很难互相沟通并且它们之间的联系也因此会越来越松散。我既不相信也不愿意这样的事情发生；在我看来，数学是一个不可分割的整体，它是一个生存能力依赖于各部分之间联系的有机体。"

1908 年罗马大会的规模超过以往历届，但绝大多数仍然是欧洲人。1912 年的国际数学家大会在英国的剑桥举行。规模有所扩大。但不久第一次世界大战开始了。国际数学家大会不得不中断。

2. 政治介入“国际数学联盟”

虽然举行了国际数学家大会，但是并没有一个常设的机构来处理国际数学界的事务。

国际数学联盟的诞生，是在国际研究理事会（International Research Council，IRC）的框架下产生的。IRC 的成立大会于 1919 年 7 月 18—28 日在比利时召开。这是一次大型会议，会上正式批准了战后国际科学政策的基本理念和实践措施。在为期 12 天的大会期间，举行了好几次全体会议，还为成立各种科学联盟而举行了大量的专门会议。会议由来自 12 个国家的 225 位代表参加。这次会议上，为筹建 IMU 召开了一次会议。该会议由比利时数学家瓦莱·普桑主持，会上作出了许多重要的决定。首先，与会者批准了带有 IRC 色彩的 IMU 章程（草稿）。选举出 IMU 的临时执委会，由瓦莱·普桑任主席，W·H·杨（英国）为副主席。会议决定国际数学家大会于 1920 年 9 月召开。

在 1920 年国际数学家大会上，来自法国、英国、意大利、比利时、美国、捷克斯洛伐克、希腊、葡萄牙、塞尔维亚、日本和波兰的代表在斯特拉斯堡大学的大厅里会面，在那里批准了一年前在布鲁塞尔会议上提出的 IMU 章程。国际数学联盟于 1920 年 9 月 20 日在斯特拉斯堡成立了。

国际数学联盟的成立，明显地具有民族主义色彩。联盟把战败的德国等同盟国的数学会排除在外。以解析函数例外值定理闻名的数学家 E·皮卡是当时的法国科学院常任秘书长。他在和英国皇家学会联系时，提出了当时协约国方面的主要问题：

“我们是否要和我们的敌人重建个人联系?”皮卡在信中表明了强烈的反对意见。作为这一方向的一个具体步骤,法国科学院将大部分的德国成员除名了。

政治从一开始就困扰着国际数学联盟。排斥战败国的并非只有法国。引进这一新政策的 1918 年伦敦会议宣言,出自英国人的笔下。但是,从一开始在英国就有反对的声音。哈代(Godfrey Harold Hardy,1877—1947)就强烈地反对歧视德国同行的做法。哈代是英国数学界的重要人物(1917—1926 年任伦敦数学会秘书长,此后两度任主席并再度任秘书长)。他说:



图 5-1　哈代

> 所有的科学联系必须完全恢复到原先的样子……考虑到英国和法国一些杰出的科学家发表了许多愚蠢的东西。我应该有必要这样说。

中立国的米塔-列夫勒强烈谴责歧视政策,毫不留情地批评了皮卡的态度。他曾同意过一种实用主义观点,认为在激情冷却之前,不邀请各同盟国国家参加国际研究理事会和各个联盟也许是明智的。不然的话,指控和争吵将搞乱所有的会议。米塔-列夫勒觉察到不仅英国和意大利有和解的愿望,即使在法国也有以阿佩尔和班勒卫为首的少数派强烈倾向和解。

德国科学家的意见是,即使章程没有禁止他们参加新的国际科学组织,他们也宁愿待在外面。他们觉得把战争的全部罪行加在他们身上的诬蔑,一个关于战争罪责的谎言,毒化了政治

气候。在正常的科学合作成为可能之前，必须完全清除那种有针对性的谴责。

1924 年的数学家大会，美国原来申请在纽约举行，并获得批准。但是到了 1922 年，由于国际数学联盟对参加者国籍的限制，使得美国各界的赞助经费落空。于是美国撤回了组织大会的申请。加拿大数学会的菲尔兹愿意在多伦多接手承办。许多参加大会的美国数学家到达多伦多后，才发现德国人被排斥在外。据说他们表示非常愤慨。在大会期间，美国代表提出一个由意大利、荷兰、瑞士、丹麦、挪威和英国附议的提案，要求国际研究理事会考虑废除目前理事会规定的限制成员国的条例。

1926 年，IRC 的态度发生变化。IMU 也随着有所改变。


图 5-2　平凯莱

平凯莱（Salvatore Pincherle，1853—1936），意大利数学家（泛函分析），国际数学联盟 1924—1928 年度主席。他作为 1928 年波仑亚国际数学家大会的主席，向不论国籍的所有的数学家打开了大门，终止了对同盟国的歧视政策。意大利的开放政策受到了广泛的赞赏。另外，丹麦、瑞士、荷兰、英国和美国都通知了大会的组织者，他们再不能容忍政治理由的歧视政策，所以，除非实行无限制的国际化，否则他们的数学家将不参加大会。

在德国，格丁根科学院要求注意这次对德国数学家的邀请，并建议给以积极回应。但是，1928 年春天，后来追随纳粹的、以单叶函数猜想闻名的 L·比伯巴赫向各大学和中学送去一封

信,催促他们抵制波仑亚大会。德高望重的希尔伯特则以自己的名义回应一封信:

> 我们相信,追随比伯巴赫先生的做法将给德国科学带来不幸,并将使我们无可辩驳地受到各方的批评……意大利同行为了伟大的理想而不嫌麻烦,花了大量的时间和精力……在当前情况下,我们应当秉持公正和基本礼节,以友好的态度对待波仑亚大会。

希尔伯特代表的观点赢得了胜利,德国人组成了除意大利人以外的最大的代表团。

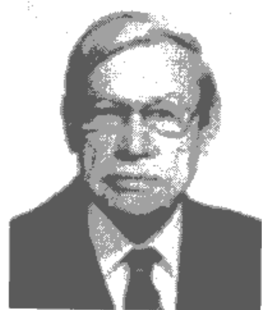
3. 第二次世界大战以后的新"国际数学联盟"

第二次世界大战结束后,西方同盟国与苏联的合作时期十分短暂。不久铁幕就把世界隔开,冷战开始了。随着殖民帝国的逐渐解体,产生了许多新的国家。这些变化也反映到了科学界。

数学界在1936年选择美国作为下一届国际大会的主办国实属幸运。于是,美国人负责在战后把全世界的数学家重新团结起来的工作。在那些年里,美国做这件事最适宜。

1946年4月在美国数学会的理事会会议上,紧急执委会报告:"只有当国际数学家大会成为一个开放的大会,使得所有的数学家都会被邀请而不管他们所效力的是哪一个国家,恢复大会的计划才有意义"。这一明确表达的美国"普遍开放宣言"对于数学来说具有重要意义。它一开始就为第二次世界大战以后的国际数学合作定下了基调。

美国数学会主席 M·斯通寄出一系列信件，收信者是各方面的群体和个人，包括阿根廷、巴西、英国、丹麦、法国、印度和瑞士的数学团体和数学家。邮寄的名单在逐步扩大，到 1949 年夏它已经包括了 26 个国家，其中包括苏联和中国。这些信件中提到新的国际数学家大会将在美国召开，新的国际数学联盟章程正在拟订之中。斯通于 1949 年 8 月寄出了章程和细则的草案。


图 5-3　斯通

章程规定，成员国的成员资格划分为 5 个等级组。划分小组有双重的意义。首先，成员国所拥有的票数等于它所属小组的等级。其次，每个成员国应该缴纳与它所属的小组相称的年度会费，标准如下：第一、二、三小组要缴纳的年费单位份额分别是 1、2、3，第四小组是 5，第五小组是 8。当时指定某一成员国在哪个小组是依据该国的人口数。现在则是当一个国家宣布要加入联盟后，由联盟根据该国的数学水平等因素综合地确定它所属的小组。

对于战败的轴心国的数学家，斯通先顺利地解决了奥地利和日本的问题。德国在战后分割为四个占领区，后来分为东德和西德。1949 年，德国数学会主席 E·卡姆克写信给斯通：

> 我听说您正在筹建国际数学联盟。想必您也会对德国数学家的参加感兴趣，我要通知您的是，德国数学会重新存在已有数年……因此，如果我们能够开始就您的计划交换意见，我将非常高兴。

斯通觉得，要给德国开绿灯需要得到国际上广泛的同意。于是他回信给卡姆克：

> 我希望在不太久的将来我们能够没有阻碍地开展这样的联系；但是就现在来说，我对您的来信的回答只能是，请耐心等待，等那些必要的准备措施完成以后。

受卡姆克来信的推动，斯通开始征求国际上对德国的意见。他的信发给了那时所有已成立的国家数学委员会（包括日本）；回答的截止期定在1950年2月1日。结果很明确，没有一个国家反对邀请德国。斯通在1950年2月2日给卡姆克的信中宣布了这一积极的结果。德国人对斯通的邀请反应迅速，很快就指定了一个全国数学委员会。

1976年，斯通写道：

> 任何人都很清楚，战争所留下的可怕的痛苦使得所有的国家都会搁置成立联盟这件事。幸运的是，有着像先在法国后到美国的曼德尔勃罗，波兰的库拉托夫斯基这样的数学家，他们本来可以愤懑地反对接纳德国，但是却反而带头公开支持接纳。

现在已没有什么力量能够阻止建立一个没有政治限制的广泛的联盟了。然而，在斯通的整个通信过程中，他没有收到一封从苏联来的回信。其他几个欧洲的社会主义国家对联盟也没有积极的反应，只有南斯拉夫例外。在欧洲，铁幕已经拉上。1953年斯大林去世后，政治气候开始变化。苏联和其他欧洲社会主义国家参加了1954年的国际数学家大会，并在1950年代末加

入了国际联盟。据报道,斯通曾这样说:

> 如果我们把联盟的工作做好了,他们(苏联和其他的东欧社会主义国家的数学家)会加入进来。如果我们做得不好,联盟就会消亡。

战后的第一次"国际数学家大会"于1950年8月30日—9月6日,在位于马萨诸塞州坎布里奇的哈佛大学举行。奥斯瓦尔多·维布伦当选为大会主席,J·R·克莱因任秘书长。1950年的大会有2 300位参加者,是以前参加人数最多一届的两倍多。在1 700名正式代表中,80%是美国人。

苏联以及东欧国家的数学家没有到会。用大会秘书长克莱因的话来说:"铁幕后的数学家由于他们自己政府的阻挠都不能来参加大会,这些政府一般拒绝发给前来参加大会数学家的护照。他们的缺席不能归因于美国政府的行为。"

政治又在干预数学活动。不过,与第一次世界大战时的情况相比,现在已有很大的不同,因为数学家在做最大的努力来推进世界范围的合作。在大会开幕之前,苏联科学院院长发来了以下内容的电报:

> 苏联科学院收到邀请苏联科学家参加将在坎布里奇举行的国际数学家大会,我们对此友善的行为十分赞赏。苏联数学家在忙于他们的日常工作,所以无法参加大会。希望即将召开的大会将成为数学科学的重要事件。愿大会取得成功。

在大会的开幕式上宣读了这份电报,其中友好的语调使人

产生今后合作的希望。这在下一届大会上得到了部分实现。

如果说1950年的国际数学家大会打上了美国的标记，那么阿姆斯特丹数学家大会标志着回到了旧世界。在1 500多名正式代表中，超过75%是欧洲人。在1954年，出国旅行还是件困难的事，所以来自欧洲和美国以外的参加者只占10%。在国家代表团中，人数最多的依次是英国261人，美国228人，荷兰212人，德国207人，法国138人。大约有1/3的邀请演讲者使用了非英语语言。这个比例在战后历届数学家大会中名列第二。在1966年莫斯科国际数学家大会上，这个比例达到55%，因为许多发言(32%)都用俄语。在1970年尼斯的数学家大会上，使用英语的比例是77%；在1994年的苏黎世大会上，这个比例是95%。

阿姆斯特丹大会有苏联数学家出席，这是他们自1932年以来首次参加ICM，所以受到特别的注意。他们的出现并非意外，因为他们已经在1953年参加了联盟主办的研讨会。虽然来的人数很少，只有5人，令人失望，但是他们的到来被看做是苏联方面表明要回到国际数学合作的意愿。

4.“在数学上，中国是统一了”

新的国际数学联盟，由于采取了正确的政策，取得了巨大的成功。但是，政治上的干涉，仍然给国际数学活动带来许多困难。

1979—1986年发生的一些政治事件，以不同寻常的力度和频度干扰了联盟的活动。1978年确定于1982年在波兰华沙举

行大会。但是,1979 年 12 月,美国与苏联之间的关系开始紧张。非政治的国际活动也受到了影响。美国决定抵制 1980 年莫斯科奥林匹克运动会,而其他一些国家却参加了,这不是个好兆头。在波兰,团结工会运动在 1980 年出现。它越来越受波兰人的欢迎,而欧洲其他大多数社会主义国家都正式表示反对。最后,在计划举行的华沙数学大会的 8 个月之前,波兰实行了军事管制。

IMU 认为,如果波兰的组织者在 1982 年 2 月答应帮助把大会转到其他地方举行,会使数学界的最大利益得到保证。但是,同从前一样,波兰人的继续施行原计划的决心十分强烈。基于这个原因,并由于时间所剩无多,转移 1982 年大会的可能性已经很小。举行华沙大会的风险得到仔细分析,最后不得不把大会推迟到 1983 年举行。

华沙数学家大会于 1983 年 8 月 16—24 日举行。总共有来自 65 个国家的 2 200 位数学家参加了大会,比前一届的赫尔辛基数学家大会少了约 1/4。与会者 1/3 以上是波兰人(830 位)。社会主义国家的参加人数不少,其中苏联人有 280 位。华人数学家丘成桐在这次会议上荣获菲尔兹奖。

下一个棘手的问题是中国代表权问题。

1978 年国际数学联盟会员全体大会表现出对中国的明显的兴趣,并通过了要求执委会继续努力使中华人民共和国成为联盟会员的决议。两个月后,一封由中华科技协会的代理主席寄给 ISCU 秘书长 John Kendrew 的信强有力地表达了北京的立场:“众所周知,世界上只有一个中国,这就是中华人民共和国;

台湾只是中国的一个省并且是她的领土的不可分割的一部分。一些国际组织的负责人把台湾省当作一个‘国家’或是一个从中国领土分离出来的‘地区’，这是我们所坚决反对的。因为它不符合事实并且完全错误，有意无意地迎合了少数人蓄意试图制造‘两个中国’或‘一中一台’的政治图谋。”

当时的IMU秘书长莱赫托在《数学无国界》一书中写道：

> 我在与中华人民共和国代表团团长吴甘美的几次讨论后的印象是，中华人民共和国将成为国际数学联盟的会员，当且仅当国际数学联盟从她的宪章中去掉“national”这一词。1985年1月底，执委会的所有委员都就我的关于中国问题的信做了回答。现在每个人都赞成向联盟会员全体大会建议从章程中删除“national”一词。

在1985年5月的执委会会议上确认了这一决定。于是IMU起草了一份详尽的备忘录，其中说明中国会员的名下有两个附属的组织：中国数学会与位于中国台北的数学会。其中第一个将有3张选票并缴纳4个单位的会费；第二个将有两张选票并缴纳2个单位的会费。

1986年7月31至8月2日在美国加利福尼亚州奥克兰举行的联盟会员全体大会之前，关于中国台北的会员国地位的问题尚不明朗。就在开幕会议的前一天，莫泽主席和莱托秘书长还在花费大量时间与他们的代表商谈。中华人民共和国代表团指出，联盟处理中国问题做得非常仔细，中国台湾的同行完全可以相信拟议中的安排绝不会以任何方式限制他们在联盟中的自

主权。他们可以在他们的所有事务中自由地使用他们学会的官方名称。莫泽和吴甘美强调,如果关于中国会籍的条款成为公开表决的结果而中国台湾又站在反对的一方,这将是多么的不幸。中华人民共和国代表团和中国台湾代表团没有取得一致意见。但在同一天晚上,在为联盟会员全体大会举行的鸡尾酒宴会中,中国台湾的代表走近莫泽和吴甘美并宣布他们决定接受联盟的命名方式。于是走完了解决问题的最后一步。联盟会员全体大会一致决定,按照执委会的 1985 年备忘录中规定的条款让中国成为联盟的会员。

这个安排的一个显著特点是:北京和台北被分在第五小组分享 5 张选票(和 5 个代表名额):北京 3 张,台北 2 张。中国台湾以前在第一小组,只有 1 张选票和 1 个代表名额,所以新的安排实际上提升了他们的地位。

这是海峡两岸数学家共同努力的结果。数学大师陈省身也在其中发挥了作用。1986 年的国际数学家大会在伯克利召开,这正是陈省身工作的地方,对中国大陆和台湾的数学家,他都可以尽地主之谊,进行沟通。另一方面,这时的国际数学联盟的主席是 J·莫泽,和陈省身是老朋友,一起合作写过论文,彼此谈话和商量事情比较方便。这些都是解决问题的极好条件。代表权问题解决之后,大家都很高兴。陈省身回忆说:“那时候,大家住在一起,都是朋友嘛。完了之后呢,到我家吃了一顿饭,大家都很融洽。至少在数学上,中国是统一了。”

参与其事的两岸数学家有:吴文俊,杨乐,程民德,谷超豪以及台湾方面的赖汉卿,刘丰哲,李国伟等。

未来之舟

国际数学联盟的工作正在有条不紊地进行。2002年，国际数学家大会在北京举行。中国数学家活跃地参与国际数学联盟的活动。随后一届的大会于2006年在西班牙的马德里举行。5.3节将介绍这次大会上获得菲尔兹奖的四位数学家的工作。印度的海得拉巴市申办2010年的大会成功。

5.2　菲尔兹奖章及其他

国际数学联盟(IMU)是全世界数学家自己的组织，它成立于1920年，其宗旨是跨越国界，推动国际数学合作。IMU的主要工作包括支持召开国际数学家大会(ICM)以及其他与数学有关的国际学术会议，还负责决定菲尔兹奖章、奈望林纳奖和高斯奖的获奖数学家人选。获奖者名单在每四年举行一次的ICM大会上公布并举行授奖仪式。

现在，还有许多以政府、组织或个人名义设立的科学大奖，它们或专门或兼顾奖励数学家的杰出工作，这些大奖对于现代数学的发展起了很好的推动作用。

1. 菲尔兹奖章

菲尔兹奖章是应加拿大数学家菲尔兹(John Charles Fields，1863—1932)的倡议而设立的。菲尔兹生前是多伦多大学的数学教授，曾在代数函数论研究中做了一些有价值的工作；但他最杰出的贡献是积极参与数学研究机构和团体的组织和管理，以此来推动数学研究事业的发展。由于他的不懈努力，创建

了加拿大国家研究委员会和安大略科学研究基金会；他担任过加拿大皇家学院1919—1925年度主席；他还成功地申请了在多伦多举办1924年ICM，并担任了该届大会的主席。


图 5-4　菲尔兹

菲尔兹因痛感第一次世界大战后同盟国与轴心国数学家之间的相互排斥和抵制危害了国际数学发展，并想弥补诺贝尔奖没有包括数学的缺憾，于是建议利用1924年多伦多ICM结余的2 500美元来设立数学奖项。菲尔兹拟订了一个详尽的计划，其中提到“通过授奖，既要表彰获奖者已经取得的成就，又要鼓励他作进一步的努力，同时对其他人也是一种新的激励”。这一想法后来被理解为只奖励年青数学家，最后被明确为获奖者不能超过40岁。菲尔兹还提出：“奖章应当具有纯粹的国际性，尽可能避免个人色彩，不能与任何国家、机构或个人的名称有任何联系。”菲尔兹未来得及实现其理想就突然病故，临终前他把价值47 000美元的遗产捐给了计划中的奖励基金。

在1932年苏黎世ICM的闭幕式上，大会宣布“以感谢的心情接受已故菲尔兹教授关于由ICM每四年颁发两枚奖章的提议”。四年后，在1936年奥斯陆ICM上第一次颁奖，它被命名为“菲尔兹奖章”以纪念菲尔兹的重要贡献，这一命名虽然有悖于首倡者本人的初衷，却得到了数学家们的一致赞同。

菲尔兹奖章用14K金制成，由加拿大雕塑家麦肯齐(Robert Tait McKenzie，1867—1938)设计。奖章(图5-5)的正面是古希

腊伟大的数学家阿基米德的侧面头像；头像右侧的一串字母 ΑΡΧΙΜΗΔΟΥΣ，系阿基米德名字的希腊文拼写；四周环绕的是拉丁文“TRANSIRE SUUM PECTUS MUNDOQUE POTIRI”，其英译文为“To transcend one's spirit and to take hold of (to master) the world”，中文可解释为“超越人的局限并把握宇宙”。据考证，此句源于古罗马诗人马尼利乌斯（Marcus Manilius，活动于公元 10 年，相当于中国西汉王莽时期）的星占学长诗 *Astronomica* 第四卷第 392 行。包含该行的那几句诗的大意为：

身为凡人并受命运摆布的占星者竟想通过观测天空来获取关于命运的知识，以寻求只有神才具有的能力，他是要超越本身的局限而把握宇宙，只有经过艰苦的努力才能取得这样的成功……

菲尔兹奖章借用这句话当然不是想把数学和占星术混为一谈，而是隐喻数学可以帮助人类超越本身的局限并了解宇宙，同时赞扬了数学家的探索求知精神。



图 5-5　菲尔兹奖章

菲尔兹奖章的背面中央也是一段拉丁文，中文意谓“从世界各地来聚会的数学家，因杰出工作而获此奖章”；拉丁文的后面

是一段月桂树枝，象征着获奖者折桂夺冠；树枝后面是一个嵌有球体的圆柱体，它代表了阿基米德最得意的定理：一个高和底面直径相等的圆柱体的体积是其内嵌球体体积的 3/2。

IMU 要为每届 ICM 任命一个由资深数学家组成的菲尔兹奖章委员会，以确定获奖者人选。著名华人数学家陈省身(1911—2004)曾当选 1962 年斯德哥尔摩 ICM 菲尔兹奖章委员会委员。根据规定，有关该委员会如何确定获奖者的文件必须封存 60 年后才能公开。

1936 年在奥斯陆 ICM 上首次获奖的是芬兰数学家阿尔福斯(Lars Valerian Ahlfors，1907—1996)和美国数学家道格拉斯(Jesse Douglas，1897—1965)。自此以后，共有 48 位数学家获得了菲尔兹奖章。其中，华人数学家丘成桐(1949—)在 1983 年华沙 ICM 上获奖。该届数学家大会原定于 1982 年召开，因波兰政局动荡实施军管而推迟了一年。获奖者的年龄都不超过 40 岁，但都被公认已做出了杰出的数学工作。解决费马大定理的英国数学家怀尔斯(Andrew J. Wiles，1953—)因年龄限制失去了获奖资格。作为补偿，1998 年 IMU 授予他特别贡献奖——一个银制的奖盘。

菲尔兹奖章常被称为“数学诺贝尔奖”，是指其荣誉与诺贝尔奖相当，但从奖金数额来讲，前者要比后者差许多。1983 年以前的菲尔兹奖章获得者每人有 1 500 加元奖金，后来因基金管理者投资有方而逐渐增加，到了 1990 年，每位获奖者可以得到 15 000加元奖金。在第二次世界大战即将结束之际，首届菲尔兹奖章获得者阿尔福斯被获准离开芬兰到瑞士苏黎世与妻子团

聚，但只被允许随身携带10克朗现金出境，他于是把奖章偷偷带出并当掉换钱，才得以摆脱经济困境，最后终于见到了妻子。这是菲尔兹奖章改变获奖者经济状况的个例。

表5-1　　历届菲尔兹奖章获得者名单

年份	获奖者(国籍)	研究领域
1936	阿尔福斯(Lars Valerian Ahlfors,1907—1996)(芬兰) 道格拉斯(Jesse Douglas,1897—1965)(美国)	极小曲面 复分析
1950	塞尔伯格(Atle Selberg,1917—2007)(挪威—美国) 施瓦尔茨(Laurent Schwartz,1915—2002)(法国)	数论 函数论
1954	小平邦彦(Kunihiko Kodaira,1915—1997)(日本) 塞尔(Jean-Pierre Serre,1926—)(法国)	代数几何 代数几何
1958	罗特(Klaus Friedrich Roth,1925—)(德国—英国) 托姆(René Thom,1923—2002)(法国)	数论 拓扑学
1962	赫尔曼德尔(Lars Hörmander,1931—)(瑞典) 米尔诺(John Willard Milnor,1931—)(美国)	偏微分方程 拓扑学
1966	阿蒂亚(Michael Francis Atiyah,1929—)(英国) 斯梅尔(Stephen Smale,1930—)(美国) 格罗腾迪克(Alexander Grothendieck,1928)(法国) 科恩(Paul Joseph Cohen,1934—2007)(美国) 汤普森(John Griggs Thompson,1932)(美国)	代数几何，拓扑学 动力系统，拓扑学 代数几何 集合论，调和分析 群论
1970	诺维科夫(Serge Novikov,1938—)(苏联) 广中平祐(Heisuke Hironaka,1931—)(日本)	拓扑学，动力系统 代数几何
1974	贝克(Alan Baker,1939—)(英国) 芒福德(David Bryant Mumford,1937—)(美国) 邦别里(Enrico Bombieri,1940—)(意大利) 费弗曼(Charles Louis Fefferman,1949—)(美国)	数论 代数几何 数论，函数论，微分方程 复变函数，调和分析
1978	马尔库利斯(Gregori A. Margulis,1946—)(苏联) 奎伦(Daniel G. Quillen,1940—)(美国)	群论 拓扑学，代数学

（续表）

年份	获奖者（国籍）	研究领域
1982	德利涅(Pierre Rene Deligne,1944—)(比利时)	代数几何
	丘成桐(Shing-Tung Yau,1949—)(中国—美国)	微分几何,偏微分方程
	瑟斯顿(William Paul Thurston,1946—)(美国)	几何学,拓扑学
	孔涅(Alain Connes,1947—)(法国)	算子代数
1986	弗里德曼(Michael Freedman,1951—)(美国)	拓扑学
	法尔廷斯(Gerd Faltings,1954—)(德国)	代数几何
	唐纳森(Simon K. Donaldson,1957—)(英国)	微分方程,拓扑学
1990	森重文(Shigefumi Mori,1951—)(日本)	代数几何
	琼斯(Vaughan Frederick Randal Jones,1952—)(新西兰)	算子代数
	威腾(Edward Witten,1951—)(美国)	物理学
	德林菲德(Vladimir Drinfeld,1954—)(乌克兰)	代数几何,物理学
1994	柴尔曼诺夫(Efim Zelmanov,1955—)(俄罗斯)	群论
	约柯(Jean-Christophe Yoccoz,1957—)(法国)	动力系统
	莱昂(Pierre-Louis Lions,1956—)(法国)	微分方程
	布甘(Jean Bourgain,1954—)(比利时)	函数论,微分方程
1998	麦克默伦(Curtis Tracy McMullen,1958—)(美国)	动力系统
	戈韦茨(Timothy Gowers,1963—)(英国)	数论,组合数学
	博切尔兹(Richard Ewen Borcherds,1959—)(英国)	数论,群论
	康切维奇(Maxim Kontsevich,1964—)(俄罗斯)	代数学
2002	拉福格(Laurent Lafforgue,1966—)(法国)	数论,代数几何
	弗沃特斯基(Vladimir Voevodsky,1966—)()	代数几何
2006	佩雷尔曼(Grigori Perelman,1966—)(俄罗斯)	微分几何
	陶哲轩(Terence Tao,1975—)(美国)	数论,微分方程,函数论
	欧克恩科夫(Andrei Okounkov,1969—)(俄罗斯—美国)	数学物理,代数学
	沃纳(Wendelin Werner,1968—)(法国)	数学物理,函数论

2. 奈望林纳奖和高斯奖

奈望林纳奖是 IMU 为纪念芬兰著名数学家奈望林纳(Rolf Herman Nevanlinna,1895—1980)于 1981 年设立的,奖金由芬兰赫尔辛基大学提供,旨在表彰在计算机科学方面作出贡献的数学家,具体包括算法理论、密码学、信息处理、程序语言、数值计算、最优控制和人工智能等领域。它和菲尔兹奖章一样,也有获奖者必须不超过 40 周岁的限制。首次颁奖是在 1983 年。



图 5-6　奈望林纳

表 5-2　　历届奈望林纳奖获得者名单

年份	获奖者(国籍)	研究领域
1983	塔尔扬(Robert Tarjan,1948—)(美国)	算法理论
1986	瓦利安(Leslie Valiant,1949—)(英国)	计算机理论
1990	拉兹波洛夫(Aleksandr Aleksandrovich Razborov,1963—)(俄罗斯)	计算复杂性理论
1994	威格森(Avi Wigderson,1956—)(以色列)	计算复杂性理论
1998	肖尔(Peter W. Shor,1959—)(美国)	量子计算
2002	苏丹(Madhu Sudan,1966—)(印度)	计算机理论
2006	克莱伯格(Jon Kleinberg,1971—)(美国)	算法理论,网络信息处理

高斯应用数学奖为纪念 19 世纪德国最伟大的数学家高斯(Carl Friedrich Gauss,1777—1855)而设立,用于奖励应用于非数学领域的杰出数学成就。鉴于数学的实用意义往往需要较长

的时间才能显现出来，所以该奖的获奖者没有年龄的限制。高斯奖由 IMU 和德国数学会联合颁发，获奖者可获得一枚奖章和 1 万欧元现金，奖金来自 1998 年柏林 ICM 大会的结余。首次颁奖是在 2006 年，获奖者是日本著名数学家伊藤清(ItôKiyosi，1915—2008)，他是概率论随机微积分学的创始人。



图 5-7 伊藤清

3. 阿贝尔奖

阿贝尔奖设立于 2002 年，正值挪威伟大的数学家阿贝尔(Niels Henrik Abel，1802—1829)诞辰 200 周年之际。阿贝尔率先证明了一般 5 次代数方程没有根式解，而法国数学家伽罗瓦(Evariste Galois，1811—1832)则在阿贝尔工作的基础上创立了群论，并给出代数方程存在根式解的充分必要条件。阿贝尔还创立了椭圆函数和代数函数的研究领域，他也是推动数学分析严密化的先驱。阿贝尔年仅 27 岁便因贫病交困而去世，当时有人称他留下的思想可供数学家工作 150 年。事实上即使在 200 年后的今天，阿贝尔在现代数学中的印记依然随处可见。



图 5-8 阿贝尔

其实早在 1897 年，挪威数学家索菲斯·李(Marius Sophus Lie，1842—1899)就曾提议设立阿贝尔奖，以弥补刚问世的诺贝

尔奖中不包括数学奖项的缺憾；当时的挪威与瑞典联合王国国王奥斯卡二世(Oscar Ⅱ，1829—1907)也已同意并开始筹划；终因挪威与瑞典联合王国在 1905 年解体而未能实施。此次设立阿贝尔奖，依然仿照诺贝尔奖的模式，每年授奖一次，奖金约 100 万美元，由挪威国王进行授奖。

挪威政府拨款两亿挪威克朗(折合约 2 300 万美元)设立阿贝尔纪念基金会，该基金除了用于颁发阿贝尔奖以及相关活动花费外，还用于关注儿童和青年的活动项目，基金会由挪威教育部负责管理；挪威科学与文学院任命一个 5 人董事会和一个 5 人数学家委员会，董事会负责安排基金的使用，委员会负责选择获奖者。基金会规定阿贝尔奖如下：

> 阿贝尔奖是一个国际奖，旨在奖励数学领域的杰出工作，包括与数学有关的计算机科学、数学物理、概率论、数值分析、科学计算、统计学领域以及数学在其他科学领域中的应用。该奖是对数学中有深远影响的卓越贡献的确认，这种贡献包括解决重大问题、创造强有力的新方法、提出统一性原理或开创新的研究领域。

表 5-3　　历届阿贝尔奖获得者名单

年份	获奖者(国籍)	研究领域
2003	塞尔(Jean-Pierre Serre，1926—)(法国)	代数几何，数论
2004	阿蒂亚(Michael Francis Atiyah，1929—)(英国)	代数几何，拓扑学
	辛格(Isadore Singer，1924—)(美国)	分析学，拓扑学
2005	拉克斯(Peter Lax，1926—)(美国)	应用数学
2006	卡尔森(Lennart A. E. Carleson，1928—)(瑞典)	复分析，动力系统
2007	瓦拉德汉(S. R. Srinivasa Varadhan，1940—)(印度—美国)	概率论

4. 沃尔夫奖

沃尔夫奖设立于 1976 年，由在以色列的沃尔夫基金会颁奖，该基金会由沃尔夫(Ricardo Subiranay Lobo Wolf, 1887—1981)夫妇创立，基金会的主席则指定由以色列教育与文化部部长担任。沃尔夫本人出生于德国，获化学博士；后移居古巴。他因发明了从熔渣中回收铁的专利技术而发财；并因全力支持古巴革命而获得与古巴领导人卡斯特罗(Fidel Castro, 1926—)的友谊；1961—1973 年，他担任古巴驻以色列的大使。1973 年以后，他定居以色列。



图 5-9 沃尔夫

沃尔夫奖旨在“奖励为人类利益和人民之间的友谊作出贡献的杰出科学家和艺术家，无论他们的国籍、种族、肤色、信仰、性别和政治观点”。科学奖励的领域包括农业、化学、数学、医学、物理学；艺术奖励则每年在音乐、绘画、雕塑和建筑领域之间轮流。每年的颁奖仪式在以色列的议会大厦举行，由以色列总统向获奖者颁奖。每位获奖者得到一份获奖证书和 10 万美元的现金；如果同一领域中有多人同时获奖，则平分奖金。

沃尔夫奖被认为是其影响仅次于诺贝尔奖的科学大奖，而且它包括了诺贝尔奖中所没有的数学、农业和艺术奖。沃尔夫奖没有对获奖者的年龄限制，因此它被认为反映了科学家的终身成就。我国农业专家袁隆平荣获 2004 年沃尔夫农业奖；著名华人数学家陈省身获 1983—1984 年沃尔夫数学奖。

表 5-4 历届沃尔夫数学奖获得者名单

年份	获奖者(国籍)	研究领域
1978	盖尔范德(Israïl Moiseevich Gelfand,1913—)(苏联)	函数论,代数学,微分方程
	西格尔(CarlS. Siegel,1896—1981)(德国)	数论,多复变函数论
1979	勒雷(Jean Leray,1906—1998)(法国)	拓扑学,微分方程
	韦伊(Andre Weil,1906—1998)(法国)	代数几何
1980	嘉当(Henri Cartan,1904—)(法国)	代数拓扑,复分析
	柯尔莫哥洛夫(A. N. Kolmogorov,1903—1987)(苏联)	概率论,动力系统,函数论
1981	阿尔福斯(Lars Valerian Ahlfors,1907—1996)(芬兰)	复分析
	扎里斯基(Oscar Zariski,1899—1986)(美国)	代数几何
1982	惠特尼(Hassler Whitney,1907—1989)(美国)	微分几何,拓扑学
	克列因(Mark G. Krein,1907—1989)(苏联)	函数论
1983—1984	陈省身(Chern Shiing-Shen,1911—2004)(中国—美国)	微分几何
	爱尔特希(Paul Erdos,1913—1996)(匈牙利)	数论,组合数学
1984—1985	小平邦彦(Kunihiko Kodaira,1915—1997)(日本)	代数几何
	卢伊(Hans Lewy,1904—1988)(美国)	偏微分方程
1986	塞尔伯格(Atle Selberg,1917—2007)(挪威—美国)	数论
	艾伦伯格(S. Eilenberg,1913—1998)(波兰—美国)	代数拓扑
1987	伊藤清(ItōKiyosi,1915—)(日本)	概率论,随机过程
	拉克斯(Peter Lax,1926—)(美国)	应用数学
1988	希策布鲁赫(Friedrich Hirzebruch,1927—)(德国)	微分几何,代数数论
	赫尔曼德尔(Lars Hörmander,1931—)(瑞典)	偏微分方程
1989	考尔德伦(Alberto P. Calderon,1920—1998)(美国)	函数论,偏微分方程
	米尔诺(John Willard Milnor,1931—)(美国)	拓扑学,几何学
1990	德·乔奇(Ennio De Giorgi,1928—1996)(意大利)	微分方程,变分法
	皮阿杰茨基-夏皮罗(Ilya Piatetski-Shapiro,1929—)(俄罗斯)	复分析,群表示论

（续表）

年份	获奖者(国籍)	研究领域
1992	卡尔森(Lennart A. E. Carleson,1928—)(瑞典) 汤普森(John Griggs Thompson,1932—)(美国)	复分析,动力系统 群论
1993	格罗莫夫(Mikhael Gromov,1943—)(俄罗斯) 蒂茨(Jacques Tits,1930—)(比利时)	拓扑学,微分几何 群论
1994—1995	莫泽(Jurgen K. Moser,1928—1999)(德国—瑞士)	动力系统,微分方程
1995—1996	朗兰兹(Robert P . Langlands,1936—)(加拿大) 怀尔斯(Andrew J. Wiles,1953—)(英国)	代数几何,群论 数论,代数几何
1996—1997	凯勒(Joseph B. Keller,1923—)(美国) 西奈依(Yakov G. Sinai,1935—)(俄罗斯)	数学物理 统计力学,动力系统
1999	罗瓦茨(Laszlo Lovasz,1948—)(匈牙利) 斯泰恩(Elias M. Stein,1931—)(比利时)	组合数学,计算机科学 傅里叶分析
2000	塞尔(Jean-Pierre Serre,1926—)(法国) 博特(Raoul Bott,1923—)(匈牙利)	代数几何 拓扑学,微分方程
2001	阿诺尔德(Vladimir I. Arnold,1937—)(俄罗斯) 谢拉(Saharon Shelah,1945—)(以色列)	动力系统,微分方程 集合论与数理逻辑
2002—2003	佐藤幹夫(Sato Mikio,1928—)(日本) 塔特(John T. Tate,1925—)(美国)	函数论,微分方程 代数数论
2005	马尔库利斯(Gregori A. Margulis,1946—)(俄罗斯) 诺维科夫(Serge Novikov,1938—)(俄罗斯)	群论,数论,代数学 拓扑学,数学物理
2006—2007	斯梅尔(Stephen Smale,1930—)(美国) 弗斯滕伯格(Harry Furstenberg,1935—)(德国)	动力系统,拓扑学,数理经济学 概率论,拓扑动力学

5. 京都奖和邵逸夫奖

京都奖被称为日本诺贝尔奖,该奖由日本稻盛基金会颁发,该基金会由日本京瓷公司创始人稻盛和夫(Inamori Kazuo,

1932—)于 1984 年捐资设立。京都奖是国际大奖，旨在“表彰那些在科学、文化和精神领域为人类福祉作出重要贡献的人”，“无论其国籍、种族、性别、年龄和信仰”。该奖分为三类奖项：先进技术、基础科学以及艺术与哲学；每类奖项原则上每年奖励一人，获奖者将得到一份证书、一枚 20K 金质奖章和 5 000 万日元现金。首次颁奖于 1985 年。其中数学属于“基础科学”门类，迄今为止有 6 人获奖。

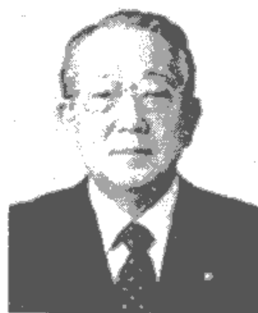


图 5-10　稻盛和夫

表 5-5　　历届京都数学奖获得者名单

年份	获奖者(国籍)	研究领域
1985	仙农(ClaudeElwoodShannon，1916—2001)(美国)	信息论
1989	盖尔范德(Israïl Moiseevich Gelfand，1913—)(苏联)	函数论，代数学，微分方程
1994	韦伊(Andre Weil，1906—1998)(法国)	代数几何
1998	伊藤清(ItoKiyoshi，1915—)(日本)	概率论，随机过程
2002	格罗莫夫(Mikhael Gromov，1943—)(俄罗斯)	拓扑学，微分几何
2006	赤池弘次(Akaike Hirotsugu，1927—)(日本)	数理统计学

邵逸夫奖由香港电影业巨子邵逸夫先生(1907—)于 2001 年设立，由邵逸夫奖基金会负责颁发。该基金会网站上如是说：

> “邵逸夫奖”为国际性奖项，得奖人应仍从事于有关的学术领域，在学术研究、科学研究及应用上有突破性的成果，或对文化艺术有杰



图 5-11　邵逸夫

出贡献，或在其他领域有卓越之成就。评选的原则主要考虑候选人之专业贡献能推动社会进步，提高人类生活素质，丰富人类精神文明。候选人近期的成果将获优先考虑。

“邵逸夫奖”现设三个奖项，分别为天文学奖、生命科学与医学奖和数学科学奖，每项奖金 100 万美元。提名及评审程序于每年 9 月开始，翌年夏季宣布颁奖典礼并于同年秋季颁奖。

“邵逸夫奖”乃国际性奖项，由“邵逸夫奖基金会有限公司”管理及执行，基金会办事处设在香港。

邵逸夫奖被称为“东方诺贝尔奖”，它并不与诺贝尔奖重复，而是要弥补诺奖的不足。

表 5-6　历届邵逸夫数学奖获得者名单

年份	获奖者(国籍)	研究领域
2004	陈省身(Chern Shiing-Shen,1911—2004)(中国—美国)	微分几何
2005	怀尔斯(Andrew J. Wiles,1953—)(英国)	数论,代数几何
2006	芒福德(David Bryant Mumford,1937—)(美国) 吴文俊(1919—)(中国)	代数几何,计算机视觉信号 数学机械化
2007	朗兰兹(Robert P. Langlands,1936—)(加拿大) 泰勒(Richard Taylor,1962—)(英国)	代数几何,群论 代数几何,数论

5.3　2006 年菲尔兹奖章获得者的数学工作

四年一度的国际数学家大会(International Congress of Mathematicians,ICM)，是由国际数学联盟(International Math-

ematical Union,IMU)支持的全世界数学家的盛会。继2002年ICM在中国北京举行之后,2006年ICM在西班牙首都马德里召开,2010年ICM则将在印度海得拉巴市举行。

历届ICM大会的主要任务包括回顾过去4年来数学研究取得的成就,展望未来发展,以及组织安排数学家之间的各种交流活动,等等;而最受全世界瞩目的一项会议内容是宣布菲尔兹奖章获得者并进行颁奖。2006年ICM宣布的菲尔兹奖章得主是:俄罗斯数学家佩雷尔曼(Grigori Perelman,1966—)、美国加州大学洛杉矶分校数学家陶哲轩(Terence Tao,1975—),美国普林斯顿大学数学家欧克恩科夫(Andrei Okounkov,1969—)和法国巴黎第十一大学数学家沃纳(Wendelin Werner,1968—)。

众所周知,佩雷尔曼获奖是由于他在证明“庞加莱猜想”中所作出的重要贡献。但由于种种原因,ICM大会给他的授奖词只字未提庞加莱猜想,而是说:

> 为了表彰他对于几何学的贡献,以及他对于Ricci流的分析结构与几何结构的革命性洞察。

更令人意外的是,特立独行的佩雷尔曼拒绝了这一象征数学家无上荣誉的金质奖章,这是菲尔兹奖章的历史上绝无仅有的事件。关于庞加莱猜想证明的百年历程以及佩雷尔曼所作的贡献,详见本书2.5节。这里介绍其他三位获奖者的数学工作。

1. 陶哲轩

ICM 2006大会给菲尔兹奖章获得者陶哲轩的授奖词:

> 为了表彰他对偏微分方程、组合论、调和分析以及

堆垒数论的贡献。

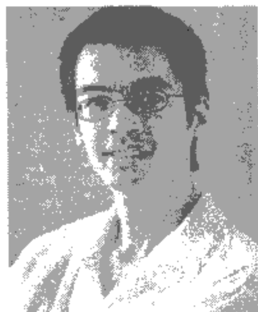


图 5-12 陶哲轩

陶哲轩是继丘成桐之后，第二位获得菲尔兹奖章的华裔数学家，不过他不是中国国籍，也不会讲一句中文。陶哲轩出生于澳大利亚阿德莱德，父母是香港移民。陶哲轩小时候是个神童。2 岁就识字，7 岁自学微积分；11 岁起连续 3 年参加中学生国际数学奥林匹克竞赛，接连获铜奖、银奖和金奖；15 岁大学毕业，21 岁获普林斯顿大学数学博士学位；目前在美国加州大学洛杉矶分校任数学教授。

曾经有不少人批评国内的数学竞赛过热，指出数学竞赛获奖并不一定就能够成为有成就的数学家。而 2006 年菲尔兹奖章的 4 位得主中竟有两位获得过数学国际奥林匹克金奖：佩雷尔曼和陶哲轩。他们的例子表明，适当的数学竞赛还是可以起到培养兴趣和发现天才的作用的。

陶哲轩被誉为解决数学问题的顶尖高手，他善于发现不同数学领域之间的联系，灵活地运用多种数学工具来攻克某个领域中的难题，并接连取得辉煌的成功；他还善于与人合作，通过与一流专家交流来获取数学知识和灵感，在他已发表的 80 多篇论文中有 30 多位合作者。陶哲轩的主要数学成就略举如下。

证明存在任意长度的等差素数列 堆垒数论是数学的传统学科，它研究满足某种加性条件的整数的性质，该领域内有着许多看似简单实则十分艰难的历史难题。其中著名的有：

华林问题 这是英国数学家华林(Edward Waring，1734—

1798)在1770年提出来的。他问是否对于任意的整数 $k \geqslant 2$,必然存在另一个正整数 s,使得每个自然数 n 都可以写成 s 个非负整数 k 次方之和。华林问题于1909年被希尔伯特解决。

孪生素数问题 所谓孪生素数是指相差为2的两个素数;比如说3和5,11和13,101和103,等等。孪生素数是否有无穷多个?这就是"孪生素数问题"。该问题迄今尚未被解决。

哥德巴赫猜想 这是德国数学家哥德巴赫(Christian Goldbach,1690—1764)在1742年提出来的。他问是否每个大于5的奇数都是三个素数之和。瑞士数学家欧拉则把这一问题改为:是否每个大于2的偶数都是两个素数之和。苏联数学家维诺格多夫(1891—1983)于1937年证明了充分大的奇数总可以表为三个素数之和。我国数学家陈景润(1933—1996)则于1966年证明了充分大的偶数总可以表为1个素数与另一个至多是两个素数乘积数之和。这是关于哥德巴赫猜想证明的目前最好的结果。

而陶哲轩与英国数学家格林(Ben Green,1977—)合作,于2006年解决了一个也有200多年历史的堆垒数论难题:

在由全部素数组成的集合中,是否存在着长度任意的等差数列?

比如说,3,5,7是长度为3,等差为2的素数列;7,37,67,97,127是长度为5等差为30的素数列。目前已知最长的等差素数列发现于2004年,它是

$$56\ 211\ 383\ 760\ 397 + 44\ 546\ 738\ 095\ 860k; k = 0,1,\cdots,22,$$

其长度为23。不难想象,要找到更长的等差素数列是非常困难

的。但陶哲轩和格林却在2006年出人意料地证明了：存在任意长度的等差素数列。也就是说，即使达到1万亿，如此长度的等差素数列也肯定存在！虽然人类可能永远不会知道这个素数列中究竟包含了哪些素数。

研究高维“挂谷问题” 日本数学家挂谷宗一（Kakeya Soichi，1886—1947）在1916年提出来一个有趣的几何问题：

怎样让平面上的一根单位长度的钢针头尾掉转180°，使得钢针扫过的区域的面积最小？

以下是使钢针掉转的几种方法。

方法1 让钢针绕其中心旋转180°。此时扫出了一个直径为1面积为$\pi/4\approx0.785$的圆（图5-13(a)）。

方法2 让钢针依次绕其两端逆时针各转60°，则3次转过后钢针正好头尾掉转。其扫过的面积为$3\times\frac{\pi}{6}-2\times\frac{\sqrt{3}}{4}\approx0.705$（图5-13(b)）。

方法3 设$\triangle ABC$是高度为1的等边三角形，钢针在AC边上且一端在A点；令钢针以A为中心旋转到AB边上，再沿着边滑行到B点；继而以B为中心旋转到BC边上，然后滑到C点；最后以C为中心旋转到AC边上，并滑回A点；这样就完成了钢针的头尾掉转。这时正好扫过$\triangle ABC$的面积$=\frac{\sqrt{3}}{3}\approx0.577$（图5-13(c)）。

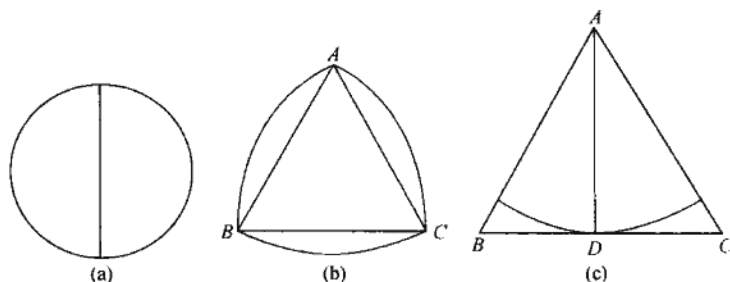


图 5-13

可见不同的方法需要扫过不同的区域面积。那么最小的面积究竟是多少呢？1928 年，苏联数学家贝西克维奇（Abram Samoilovitch Besicovitch，1891—1970）给出了一个出人意料的最终答案：使钢针掉头而需要扫过的区域面积可以任意地小。贝西克维奇证明方法的要点在于每次使钢针转动尽可能小的角度，并且让钢针在两次转动之间沿直线来回滑动相当长距离，从而使每次转动的区域尽可能重叠起来。贝氏方法使得钢针扫过的区域形成了一种形状奇特的平面图形，被称为“贝西克维奇集合”，该集合的勒贝格测度趋于零，而且其“闵科夫斯基维数”等于 2。

把挂谷问题和贝西克维奇集合推广到高维空间有多种方法。比如说，考虑有一定截面积的单位长度铁棒在空间中转过所有的方向，求所需扫过空间的最小体积以及“闵科夫斯基维数”。高维挂谷问题极其困难，但近几年人们对它兴趣大增，因为发现它与多个数学分支有关，如数论、组合学、傅里叶分析、周期积分、扩散方程和波动方程等。陶哲轩在高维挂谷问题研究及应用中获得一系列重要结果，被公认为是该领域的领头人物。

其他成就　陶哲轩还在解圆柱对称爱因斯坦引力方程方面

取得进展,这类方程曾被认为是无法求解的。他带领其他 4 位数学家组成"团队",合作解出了描述光纤中光传播的非线性薛定谔方程。他还与人合作证明了关于两个埃尔米特矩阵和的特征值分布的著名的"霍恩猜想";人们惊叹一位纯粹数学家竟在应用数学领域做出了如此重要的工作,形容说就好像看到一位英语小说的一流作家突然写出了一部精彩的俄文小说。

2. 欧克恩科夫

ICM 2006 大会给菲尔兹奖章获得者欧克恩科夫的授奖词:

为了表彰他为建立概率论、表示论和代数几何之间的联系而作出的贡献。



图 5-14　欧克恩科夫

欧克恩科夫 1969 年出生于苏联莫斯科,1995 年获莫斯科国立大学博士学位;他曾在俄罗斯科学院、美国普林斯顿高级研究所、芝加哥大学和加利福尼亚大学贝克莱分校等处任职,目前是美国普林斯顿大学的数学教授。

欧克恩科夫的工作揭示了:置换群的表示论、组合学、随机矩阵和代数几何这几个看上去不同的数学领域之间存在着深刻的联系,而这些联系又与量子场论、统计力学和弦论这些物理学科领域密切相关。

给定 n 个对象,它们的一个置换就是这些对象的一个有序排列,比如说,给定 A,B,C,D,E,F,G,H 这八个(字母)对象,$ABCDEFGH$ 和 $HGFEDCBA$ 是它们的两个不同置换。n 个对

象的所有置换构成了一个置换群：组合论基础知识告诉我们，这个群里共有 $n! = n \times (n-1) \times \cdots \times 3 \times 2 \times 1$ 个元素。数学家经常通过把各种群映射到矩阵上以研究其种种性质，这就是群表示论。而置换群表示论不仅本身是一重要的数学分支，而且在量子力学等其他学科领域有重要应用。

研究表明，置换群的基本结构可以用整数的“分拆”(即拆成若干个整数之和，如整数 24 有一个分拆 1+3+3+5+12)来区分。这就建立了置换群表示论与另一个古老的数学分支——组合论——之间的联系。由于置换群元素个数随着被置换对象个数 n 的增加而迅速增加，反映到组合论中，就是一个极大数的分拆问题了。苏联的数学家早在 20 世纪 70 年代，就开始用概率论的方法来研究这种分拆问题。欧克恩科夫则继承了这一传统，在此研究中取得了惊人的成功。

他的一个早期研究成果与“随机矩阵”有关。随机矩阵是元素为随机数的方阵，它在物理学中有广泛应用。欧克恩科夫借用量子场论中的思想，出人意料地证明了随机矩阵的特征值与对象为整数的置换中的递增子序列之间存在深刻的关系。他在证明中首创了“随机曲面”的概念，而这又和代数几何这个数学分支建立了联系。

欧克恩科夫与他人合作，利用“随机曲面”解决了统计力学中的一个问题：设想一个物理晶体，其边角在慢加热中逐渐溶解。从几何的角度，可以把此溶解过程看成是不断地随机地取走晶体边角上的小块；从组合论的角度，可以把晶体的边角看做一个整数而把那些小块看做是它的分拆。欧克恩科夫及其合作

者令人惊讶地发现，晶体边角在溶解过程中形成的随机曲面的二维投影是一条代数曲线，即它可以用一个多项式方程来描述。这条代数曲线就是人们熟知的“心脏线”(图 5-15)。

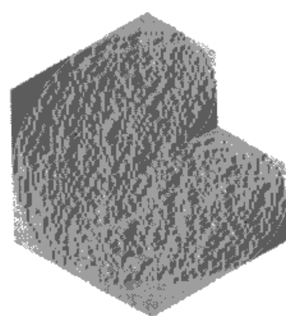


图 5-15　晶体边角溶解过程中形成的随机曲面二维投影是“心脏线”

欧克恩科夫与他的合作者最近几年一直专注于“计数代数几何学”的研究。计数代数几何学研究如何给一组多项式方程加上适当的条件，比如说改变它们的系数或令它们通过给定的点，使得它们正好代表了有限条代数曲线。加的条件太强可能得不到一条曲线，条件太弱则会产生无数条曲线。这类“曲线计数”问题不仅是代数几何学的长期研究课题而且与近几年大热的“弦论”密切相关。欧克恩科夫及其合作者巧妙地把物理学思想和大量的不同数学领域的工具结合在一起，取得了不少研究成果。他们的工作代表了数学和物理学之间神奇的相互作用。

3. 沃　纳

ICM2006 大会给菲尔兹奖章获得者沃纳的授奖词：

> 为了表彰他为发展随机共形映射、二维布朗运动几何学以及共形场论所作的贡献。



图 5-16　沃纳

沃纳 1968 年出生于德国，1977 年加

入法国籍，1993 年获法国第六大学博士学位，1997 年起任巴黎第十一大学数学教授。

沃纳与其合作者的工作代表了近年来数学和物理学之间富有成果的交互作用的最精彩的部分。他们运用概率论和复分析，为理解物理中的临界现象建立了一种新的概念框架。物理世界的各种分子系统中经常发生各种相变，如水结冰、液化和气化以及铁的磁性排列随温度改变，等等；发生相变的那一刻叫做临界现象，它一般只与温度有关，而与尺度无关；这种现象由于涉及巨量分子的无规则运动而极其复杂，人们对它了解甚少。经过包括一些诺贝尔奖获得者的物理学家们的长期努力，终于在 20 世纪 90 年代发展了一种叫做“共形场论”的理论，可以用来解释二维临界现象。但这个理论从数学的角度来看是不严格的，并且它无法提供有关临界现象的直观的几何图像。而沃纳与其合作者的工作彻底改变了这种局面。

有一类二维临界模型是平面涂色铺砖模型：想象在一个坐标平面上铺满了六角形砖，在每块砖上以概率 p 涂黑色，以概率 $1-p$ 涂白色。要问在平面的哪些地方存在着完全由黑色砖铺成的通往坐标原点的路径(图 5-17)？这样的路径形成了一个个串，这些串具有分形结构。物理学家们大量利用这类模型来研究渗流，预测其中的临界现象：渗流是自然界一种常见现象，如水在管道网络中的渗流和污染物的扩散，等等。沃纳与其合作者则运用严密的数学理论，通过让六角形砖不断地缩小而获得了这类模型的许多重要性质，包括它的分维数和临界指数，等等。

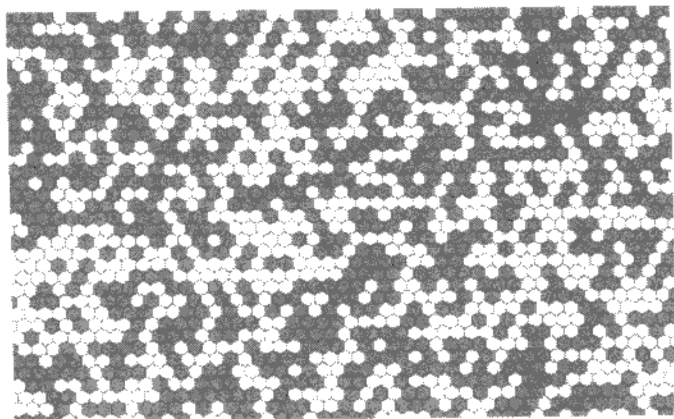


图 5-17 此随机铺砖图中存在哪些由黑色砖铺成的路径

另一个二维临界模型是平面布朗运动，即分子的平面随机运动。布朗运动的几何图像极其复杂，但可以确定其具有分形结构，人们很早就猜测它具有分维数 4/3，却一直无法证明它。后来终于被沃纳及其合作者所证明。

沃纳及其合作者还证明了一些二维模型的“共形不变性”，即这些模型在复分析的共形映射下保持不变。“共形不变性”在共形场论中被当作是一种重要的基本性质，它假设大多数模型都具有这种性质，并以此作为研究的出发点。

沃纳及其合作者的工作大大增进了人们对二维临界现象的了解，加深了数学和物理之间的联系和沟通，并开创了充满机会的新研究领域。

未来之舟

从 19 世纪开始，数学逐渐发展成为一门高度抽象且分支繁多的学科：它不仅独立于现实世界以及其他科学，有着自己独特的研究对象和研究方法；而且不同分支之间的差异甚大，以至许多数学家只能掌握自己狭小领域的那些专门知识，而对其他数学分支几乎一无所知。但 20 世纪 90 年代

以来，数学的发展呈现重新统一的趋势，这从 2006 年菲尔兹奖章获得者的工作中也能看出。首先，数学与其他科学尤其是物理学之间的相互影响越来越大，大量抽象的数学工具被用于各种科学领域，由此产生了一系列新课题和新领域，吸引了包括数学家在内的许多研究者。其次，纯粹数学与应用数学之间也在相互渗透，有时已经分不清哪些属于纯粹数学哪些属于应用数学。最后，即使在纯粹数学中，那些曾经相互独立的分支，如代数、几何、分析、数论等等，现在也融合起来；我们看到，几乎每一个重大数学问题的解决都需要综合运用多门数学工具。在这种形势下，像陶哲轩、欧克恩科夫和沃纳那样具有横跨多门数学领域的知识或通晓其他科学的卓越数学家就会如鱼得水，不断取得创造性成果。

5.4　克莱新千年奖

——从希尔伯特 23 个问题到 21 世纪数学问题

在一个世纪的开端，预测未来百年应该解决的数学问题，是一个令人心仪的事件。1900 年，希尔伯特提出的 23 个数学问题，曾经激励着全世界的数学家努力攀登，展现人类的智慧与才智。当 2000 年到来的时候，又有一张未解决的数学问题清单问世，其中每个问题都悬赏 100 万美元。

1. 希尔伯特以提出 23 个问题作为大会演讲



图 5-18　希尔伯特

1900 年 8 月 6—12 日，第二届国际数学家大会（ICM）在法国巴黎召开。8 月 8 日那一天，38 岁的德国数学家希尔伯特意气风发地走上大会讲台，他要在全世界数学家的瞩目之下，大胆地预测 20 世纪的数学

发展。他开始道：

> 谁不想揭开遮着未来的帷幕，窥探今后百年我们这门科学前进和发展的秘密？下一代的数学主流将会追求什么样的目标？新世纪将会给广阔丰富的数学思想带来何种新方法和新成果？

希尔伯特认为，展望数学未来的最好方法是考查那些尚未解决的数学问题。

> 历史教导我们，科学是延续发展的。每个时代都有自己的问题，这些问题或者被后代解决，或者因为无所获益而被他们丢弃并代之以新的问题。如果我们想要把握数学最近的发展趋向，就必须想想有哪些尚未解决的问题，特别要考查那些当今科学提出的并期望将来能解决的问题。值此世纪更迭之际，我认为正适于对现有的问题进行这样一番检阅。因为一个伟大时代的结束，不仅要让我们回顾过去，更要把我们的思想引向那未知的将来。

希尔伯特进一步指出数学问题对于数学发展的重要意义。

> 数学问题对于数学总体进步具有深刻的意义，并且在数学家个人工作中起着重要作用，这是不容否认的。只要一门科学分支能够提出大量的问题，它就充满着生命力；而问题缺乏则预示着衰亡或停止发展。正如人类的每项事业都追求着确定的目标一样，数学研究也需要有自己的问题。正是通过解决问题，研究

者得以考验其毅力，发现新方法和新观点，并达到更为广阔和自由的境界。

但是，并非所有的数学问题都值得认真对待。希尔伯特提出了判断准则。他认为一个好的数学问题应该清晰易懂，以至可以向大街上遇到的任何人解释它；此外，它应该有相当的难度从而能够引诱人们来接受挑战，但又不是完全不可解决以至让人们白费精力。

根据上述思想和原则，希尔伯特提出了涉及当时几乎所有重要数学领域的 23 个问题，期望 20 世纪的数学家能够获得它们的答案。

转眼之间，20 世纪已经过去。回顾这 100 年的数学发展，是如此的波澜壮阔、丰富多彩，远远超出了世纪之初任何人之想象。即使是希尔伯特，当初他也肯定没有料到其法国同行庞加莱会在 4 年之内开创一门崭新的学科——拓扑学，它将占据 20 世纪纯粹数学的中心舞台；也不曾想到，物理学的相对论和量子力学会在二十几年中相继问世，它们将强有力地推动数学微分几何与泛函分析的研究；更不能预见，人类会在 50 年内遭受两场世界大战的浩劫，但战争促使了应用数学以及计算科学的兴起，而后两者在 20 世纪后半叶的繁荣和发展甚至改变了以纯粹数学为中心的数学领域传统格局。

尽管如此，希尔伯特的 23 个问题依然在 20 世纪的数学中占有无可争议的地位。数学家们都以能够解决或推动解决其中一个问题为极大的荣誉。经过这 100 年，大部分问题已经获得解决，虽然有些问题的答案与希尔伯特当初所期望的有所不同

甚至正好相反。无论获得解答与否，对于这些问题的深入研究是20世纪数学发展的一个重要推力。从这一点来说，希尔伯特当年的愿望已达到。

2. 希尔伯特问题的进展综述

以下对希尔伯特23个问题中1～17个问题略作介绍。其中问题1～6是关于数学基础的；问题7～12涉及数论；问题13～17属于代数几何或代数领域。

问题1 *康托的连续统假设* 这是指由集合论的创立者，德国数学家康托(Georg Cantor，1845—1918)提出的猜测：

> 实数集合中的任何无穷子集或者与自然数集等价或者与整个实数集等价。

1963年，美国数学家科恩(Paul Joseph Cohen，1934—2007)证明了连续统假设不可能在策梅洛-弗兰克尔公理化集合论系统(简称Z-F系统)中被证明或否证。Z-F系统是最接近实际数学的形式化数学系统(参见本书3.6节的介绍)。所以，科恩在某种意义下解答了希尔伯特的第一个问题，他因此于1966年荣获菲尔兹奖章。

问题2 *算术公理系统的相容性证明* 这里的算术公理，其实指建立在集合论基础上的实数理论；而所谓系统的相容性，是指该系统中不存在两个互相矛盾的定理。1931年，奥地利数学家哥德尔(Kurt Gödel，1906—1978)证明：

> 任何一个包含自然数的集合论公理化系统不可能既是完备的又是相容的。

实数系统当然包含自然数。因此，哥德尔的定理实际上是说算术公理系统的相容性无法证明(参见本书3.5节)。

问题3 *不可能把任意两个同底同高的四面体剖分为全等的有限部分* 我们知道，同底同高的两个四面体的体积相等。但这一事实是通过“无限分割”的极限方法证明的。那么，有无可能用非极限方法来证明呢？比如说，把这两个四面体分别切成几块，使得各块的形状大小分别相同(全等)，这就证明了它们总的体积相等。希尔伯特认为这种方法行不通，即存在不能进行这样剖分的两个四面体。这一问题在提出的当年(1900年)就被希尔伯特的学生德恩(Max Dehn，1878—1952)解决，他构造了不能进行剖分的两个同底同高的四面体。

问题4 *构造以直线为两点间最短距离的所有的几何体系*

我们知道欧几里得几何其实是一个由一组公理规定的逻辑推理体系。如果改变了其中的公理就会得到不同的几何。比如说，改变平行公理可以得到“双曲几何”或“椭圆几何”。希尔伯特现在提出，如果把“两点之间最短距离是直线”作为公理，同时允许改变其他公理，那将可能得到怎样的几何？他认为这一问题不仅在几何学而且在数论和变分学中有重要应用，对于它的研究还将有助于我们更好地理解“距离”和“平面”等几何概念。这一问题迄今尚未解决。

问题5 *连续变换群是否一定是可微的* 所谓变换群是指一组满足“群运算”规则的几何坐标变换方程。挪威数学家索菲斯·李(Marius Sophus Lie，1842—1899)率先研究这种群，不过他总是假设它们是连续的和可微的。后来，“可微的变换群”就

被称为“李群”。李群在许多数学领域以及在物理学领域有重要的应用(参见本书1.4节)。希尔伯特认为“可微性”并不是一个自然的几何概念。于是他问,能否从变换群的连续性推出它们的“可微性”,从而可以省略李群中的“可微性”假设呢？1952年,美国数学家格里森(Andrew Mattei Gleason,1921—)等人给出了这个问题的肯定解答。

问题6　*物理学的公理化*　希尔伯特建议像建立几何学公理化体系那样,建立起物理学的公理化体系。他特别提到了概率论(主要涉及分子运动)和力学的公理化。概率论的公理化已于1933年由苏联数学家柯尔莫哥洛夫(Андре́й Никола́евич Колмого́ров,1903—1987)完成(参见本书3.1节)。至于力学以及其他数理学领域的公理化。由于相对论和规范场理论的先后出现,使得“对称性”几乎成为物理学的基本概念,并使得微分几何与群论等数学分支成为物理学研究的主要工具。因此可以说,物理学的公理化有相当的进展,但距最后的完成还有很漫长的路要走。

问题7　*关于某些数的无理性和超越性*　所谓无理数是指不能写成分数形式的实数,可表为某个有理代数方程之根的数被称为“代数数”,超越数则是不能表为任何有理代数方程之根的实数。比如说,$\sqrt{2}$是无理数也是代数数;而自然指数e和圆周率π均为超越数。希尔伯特提出,形如α^{β}的数(其中α为代数数,β为无理数)都是超越数。他认为这是一个极其困难的问题,需要有全新的观点和方法才有可能解决。然而苏联数学家盖尔封特(Alexander Gelfond,1906—1968)于1934年,德国数学家

施奈德(Theodor Schneider,1911—1988)于 1935 年分别独立地解决了这个问题。答案是肯定的。

问题 8　*素数问题*　希尔伯特在此指出,有关素数分布的彻底解决有赖于"黎曼猜想"的证明;而在搞清了素数分布之后,就可以解决"哥德巴赫猜想"和"孪生素数猜想"等问题。但到目前为止,这些猜想都没有得到解决。

问题 9　*关于任意代数数域的一般互反律的表示及证明*　整数域的二次互反律是关于任意两个奇素数之间"二次剩余"关系的一个重要定理,在古典数论中有广泛应用。希尔伯特因此想把它推广到一般代数数域。日本数学家高木贞治(Takagi Teiji,1875—1960)和德国数学家阿廷(Emil Artin,1898—1962)部分解决了这一问题。

问题 10　*关于丢番图方程可解性的判别*　所谓丢番图方程是指要求整数解的那些整系数代数不定方程,如我国古代的"百鸡问题"和"费马大定理"所涉及的方程都属于此类,因古希腊数学家丢番图(Diophantus,活动于约公元 250 年)率先研究而得名。希尔伯特希望有一种程序,能够在有限步骤内判定一个丢番图方程是否存在整数解。1970 年,苏联数学家马季亚谢维奇(Yuri Matiyasevich,1947—)证明了这种程序不可能存在,因而否定地解答了这一问题。

问题 11　*求解系数是代数数的二次型方程*　此问题已被部分解答。

问题 12　*把关于有理数域上阿贝尔扩张的克罗内克定理推广到任意代数数域*　希尔伯特认为此问题与问题 9(关于一般代

数数域的互反律)有密切联系。尚未有解答。

问题 13　是否可能利用一些二元函数来求解一般 7 次代数方程　我们已经知道,5 次及以上的代数方程一般没有根式解。但可以证明,5 次和 6 次代数方程的根可以表为一些二元函数的复合。那么,7 次及以上的代数方程的根能否也表示为一些二元函数的复合呢?希尔伯特猜测答案是否定的。然而在 1957 年,年仅 19 岁的苏联数学家阿诺尔德(Vladimir Igorevich Arnold,1937—)却证明了,任意的多元连续函数总可以表示为有限个二元连续函数的复合,从而肯定地解答了这一问题。

问题 14　证明一些完全函数系统的有限性　特别地,希尔伯特希望能够证明有理函数域上的一些环结构是有限生成的。但在 1958 年,日本数学家永田雅宜(Nagata Masayoshi,1927—)给出了一个反例,从而给出了这个问题的否定答案。

问题 15　给出舒伯特计数演算的严格基础　德国数学家舒伯特(Hermann Schubert,1848—1911)发展了计算诸如“相交数”之类几何量的方法,因此创立了“计数几何”。希尔伯特要求为它建立起严格的逻辑基础。计数几何目前是代数几何的一个分支,但其基础问题尚未完全解决。

问题 16　关于代数曲线和曲面的拓扑结构　希尔伯特在此其实要求解决两个问题,一个是研究代数曲线(曲面)各闭分支的相对位置;另一个是求出由一类一阶常微分方程确定的向量场极限环个数的上界。这些问题都尚未解决。

问题 17　关于正定形式的平方表示　一个实系数的任意元有理函数被称为是正定的,如果它在实数定义域上总是取非负

值。如果这个函数只包含二次项，就称它为正定(二次)形式。希尔伯特问道，正定形式是否总可以表为两个平方形式的商？1927年，阿廷给出了肯定的解答。

问题18—23涉及几何、微分方程、函数论和变分法等领域，在此省略。

3.21世纪面临的问题

对于人类来说，公元2000年具有特殊意义，因为这一年不仅标志着20世纪的过去和21世纪的到来，也意味着公元第二个千年的终结以及第三个千年的开始。每当送旧迎新之际，人们总会对新的未来有所猜测和期盼。那么，数学家对于新世纪和新千年的数学又有什么期待呢？他们记住了100年前希尔伯特所说的那些话和所提出的23个问题。2000年5月24日，美国的克莱数学所(Clay Mathematical Institute)专门来到法国巴黎的法兰西学院召开"新千年会议"。会后郑重宣布：

> 为了庆祝新千年的数学，克莱数学所设立了七个"获奖数学问题"。这些问题由数学所的科学顾问会选出，它们都是长期未能解决的重要的"经典数学问题"。数学所董事会拨出了700万美元奖金，解决每个问题获100万美元奖金……
>
> 100年前的1900年8月8日，大卫·希尔伯特在巴黎举行的第二届国际数学家大会上发表了关于数学问题的著名演讲，这促使我们决定来到巴黎举行"新千年会议"并宣布"新千年数学问题"……

克莱数学所成立于 1998 年，位于美国马萨诸塞州坎布里奇市，由波士顿商人克莱夫妇（Landon T. Clay&Lavinia D. Clay）斥资建立，是一个非盈利性质的私人机构；克莱本人任数学所主席，并由克莱家族组成董事会；但负责学术事务的数学所所长和科学顾问会成员都是著名的数学家。克莱数学所规定的主要工作包括：增进和传播数学知识，向数学家和其他科学家通报数学领域的新发现，鼓励天才学生从事数学事业，以及嘉奖数学研究中取得的杰出成就和进步。

列入“克莱新千年数学问题”名单的分别是：庞加莱猜想、黎曼猜想、伯奇和斯温纳顿-戴尔猜想、杨-米尔斯理论、纳威尔-斯托克斯方程、霍奇猜想、P-NP 问题。

庞加莱猜想是法国数学家庞加莱（Henri Poincaré，1854—1912）在 1904 年他的拓扑学开创性论文中提出来的。他问：

> 一个闭的三维几何图形，若其上的每条闭曲线都可以连续收缩到一个点，那么从拓扑上来看，这个图形是否一定是球面？

该猜想一直是拓扑学研究的中心课题，曾经顽强地经受了数学家们整整 100 年的轮番冲击。但是到了 2006 年，数学家公认庞加莱猜想已被证明，关于其证明历程参见本书 2.5 节“破解拓扑学世纪之谜”。

庞加莱猜想成为第一个被解决的“克莱新千年数学问题”。然而，第一笔“新千年数学奖”怎样颁发？这看来已成为克莱数学所自己的难题了。因为根据当初的规定，任何解决了新千年问题的成果都必须正式发表在世界著名的数学刊物上，并且在

两年之后得到数学界广泛承认，数学所才会考虑颁奖。但为解决庞加莱猜想作出主要贡献的俄罗斯数学家佩雷尔曼(Grigori Perelman，1966—)在 2002—2003 年把他的三篇关键论文非正式地发表在因特网上。而且佩雷尔曼已经拒绝了菲尔兹奖章。人们猜测，如果宣布把新千年奖授予他，是否也会遭到拒绝呢？

黎曼猜想属于希尔伯特 23 个问题中的遗留问题，这在新千年数学问题中是唯一的。自从费马大定理和庞加莱猜想被相继证明之后，黎曼猜想已被公认为是纯粹数学中最重要和最困难的问题了。据传希尔伯特曾经说过："如果我在沉睡了 1 000年后醒来，我的第一个问题会是，黎曼猜想被证明了吗？"也许他已经预感到需要花 1 000 年时间才能证明黎曼猜想。



图 5-19　黎曼

那么，黎曼猜想究竟是怎么回事？这要从 18 世纪数学家欧拉(Leonhard Euler，1707—1783)发现的一个关于素数的奇妙公式说起。这个公式是

$$\prod_p (1-p^{-s})^{-1} = \sum_{n=1}^{\infty} n^{-s}。 \tag{1}$$

其中，$\prod\limits_p$ 表示对每一个素数的连乘，即

$$\prod_p (1-p^{-s})^{-1} = (1-2^{-s})^{-1}(1-3^{-s})^{-1}(1-5^{-s})^{-1}\cdots,$$

而 $\sum\limits_{n=1}^{\infty}$ 表示对每一个自然数的连加，即

$$\sum_{n=1}^{\infty} n^{-s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots。$$

根据无穷级数和无穷乘积的知识，当 $s>1$ 时，式(1)的两边都收敛于有限的实数，因此相等。欧拉利用这一公式，很简单地证明了素数不仅有无限多个而且在自然数中相当稠密。他甚至算出了当 s 为偶数时式(1)的具体数值。

1859 年，德国数学家黎曼(Georg Friedrich Bernhard Riemann，1826—1866)在其著名的论文“论小于给定数的素数个数”中，把式(1)定义为函数 $\zeta(s)$(其中 ζ 是希腊字母，念做 zeta)。他令 s 取复数，并证明了 $\zeta(s)$ 可以延拓成整个复平面上的解析函数，除了 $s=1$ 为极点。黎曼在研究了 $\zeta(s)$ 的一系列性质之后，提出了他的猜测，其意思说(并非原话)：

$\zeta(s)$ 的所有非平凡零点很可能都在复平面的过实轴 $x=\frac{1}{2}$ 点并与虚轴平行的那条直线上。

这就是黎曼猜想！利用这一猜想，黎曼很容易地获得了素数公式。

黎曼猜想因为与数论的中心问题——素数分布——有密切的联系，所以从一开始就受到了高度重视。100 多年来，数学家从各个方面向它发起冲击，却无多大进展。有人利用计算机，验证了 $\zeta(s)$ 的前 15 亿个零点都符合黎曼猜想，但这代替不了证明。

1896 年，法国数学家阿达马(Jacques Hadamard，1865—1963)等人绕过黎曼猜想，证明了素数分布定理。但这并没有使黎曼猜想的价值降低。因为黎曼猜想可以给出素数公式误差项更精确的估计。而且，它还能给解决哥德巴赫猜想和孪生素数

猜想等著名数论难题提供很大的帮助。另外，黎曼猜想在代数数域和有限数域中有各种推广。因此可以说，黎曼猜想的重要意义已经不仅限于数论，而是涉及整个纯粹数学领域。

黎曼猜想在有限数域上的推广首先由法国数学家韦伊(André Weil，1906—1998)提出，因此被称为“韦伊猜想”。对于该猜想的研究是代数几何现代发展的主要推动力。令人惊讶的是，比利时年轻数学家德利涅(Pierre Rene Deligne，1944—)于1973 年证明了韦伊猜想。这被认为是 20 世纪的主要数学成就之一。德利涅因此在 1978 年获得了菲尔兹奖章。

伯奇和斯温纳顿-戴尔猜想由英国数学家伯奇(Bryan John Birch，1931—)与斯温纳顿-戴尔(Peter Swinnerton-Dyer，1927—)在 1965 年提出。该猜想用通俗的话来叙述，就是

有理数域上椭圆曲线的 L-函数零点的阶正好等于该曲线上有理点群的秩。

我们知道，形如

$$y^2 = Ax^3 + Bx^2 + Cx + D \tag{2}$$

的代数方程被称为“椭圆曲线”(参见本书 2.4 节)；当式(2)中的系数 A,B,C,D 都是有理数时，就称该曲线是“有理数域上的”；而“L-函数”则是黎曼 ζ-函数在代数方程解空间上的一种推广。

我们在 2.4 节中已经介绍，椭圆曲线是代数几何领域中最简单也是最重要的研究对象。著名的费马大定理问题就是通过证明了关于“椭圆曲线上的 L-函数都是模形式”的谷山-志村-韦伊猜想而得到解决的。而伯奇和斯温纳顿-戴尔猜想则又把椭圆曲线的 L-函数与其有理点(即曲线的有理数零点)群的结构联

系起来。如果此猜想得以证明，将使数学家对于椭圆曲线的性质有更一般更深入的了解，从而可以帮助解决一大类代数几何的难题。

杨-米尔斯理论得以进入克莱新千年数学问题的名单，充分显示了现代物理学研究对于现代数学发展的重要影响(参见本书3.3节)。克莱数学所关于此问题的完整叙述是：

> 证明对于任何紧致单规范群，在四维欧氏空间上存在一个质量间隙大于零的非平凡量子杨-米尔斯理论。

本书1.4节“对称、守恒、规范场与群论”中已介绍，物理学家杨振宁和米尔斯于1954年创立的“非交换规范场理论”已经成为描述电磁力、弱力和强力作用的标准模型。其中强作用力的规范场理论又叫做“量子色动力学”(quantum chromodynamics，简记QCD)，它能够相当精准地刻画量子尺度的物理现象。然而，QCD并非是一个纯粹的数学理论，它其实需要一些物理上的假设条件，特别是依赖于以下三个条件。

(1)存在“质量间隙”，即一个大于零的常数质量值，只有当真空的能量大于等于该值时才可能产生“激发”；

(2)“夸克幽禁”，即作为QCD中最基本的粒子“夸克”，它们总是被束缚在一起，无法单独分开，因此人类永远观察不到单个的夸克；

(3)“手征对称破缺”，即真空在规范群的作用下并不能完全保持不变。这三个条件都已经被各种物理实验所证实，但是目前还不能从数学上解释它们。

我们所能观察到的物理世界正好是四维的(三维空间加一维时间),如果数学家们真能够建立起关于四维欧氏空间的非平凡量子杨-米尔斯规范场理论,并且能够解释以上三个条件,那将不仅会加深我们对于现实物理世界的了解,还会促进现代数学思想的发展。这就是克莱数学所把杨-米尔斯理论列入其“新千年数学问题”的主要理由。

纳威尔-斯托克斯方程是描述流体(包括气体和液体等)运动的一组非线性偏微分方程,它首先由法国工程师和物理学家纳威尔(Claude-Louis Navier,1785—1836)于 1821 年得到,又被英国数学家和物理学家斯托克斯(George Gabriel Stokes,1819—1903)在 1845 年重新发现,因而以他们两人的姓命名。纳威尔-斯托克斯方程的应用领域极其广泛,如用于描述大气层气流运动、海洋中洋流运动、管道气体或液体流动、动物体内血液流动、宇宙星体运动,还可用于磁流体力学,甚至是经济学领域,等等。制造飞机、汽车、火车、轮船以及气象预报,都离不开此方程。

令数学家们汗颜的是,对于如此重要的方程却至今不能求出它的分析解,甚至连解的存在性都无法证明。目前科学家和工程师们都是通过风洞实验和计算机模拟的方法来获得纳威尔-斯托克斯方程的数值解,以解决实际应用问题,并收到很好的效果。这说明该方程的解肯定存在,但用通常的处理偏微分方程的数学分析方法却得不到它。数学家已经认识到,只有发展新思想和新方法才有可能改变这一尴尬的局面。

此次克莱数学所把证明纳威尔-斯托克斯方程在三维欧氏

空间中存在光滑解作为“新千年数学问题”之一。因为他们相信,该问题的解决无论对于科学技术进步还是对于数学本身发展都具有极其重要的意义。

霍奇猜想是英国数学家霍奇(William Hodge,1903—1975)在1950年国际数学家大会(在美国哈佛大学举行)上提出的。该猜想用现在数学的语言表述,就是

设 X 是一个复射影代数簇,则 X 的每个“霍奇类”都是 X 的“代数闭链”的线性有理组合。

其中“复射影代数簇”指的是由一组复系数齐次代数方程的零点所形成的流形,“霍奇类”是 X 上通过一系列微分运算得到的一种整体拓扑性质,而“代数闭链”则是由 X 的子簇所代表并通过子簇上的积分运算来定义的另一类 X 拓扑量。

霍奇猜想如果成立,则提供了利用“代数闭链”研究代数簇整体性质的理想途径。计算“代数闭链”有多种方法,特别是它还与另一个流形上重要的不变量“陈(省身)类”有密切的联系。

霍奇猜想属于代数几何领域,但它所涉及的概念与微分几何、拓扑学、代数学和分析学等其他数学领域都有关。因此,该猜想反映了纯粹数学不同分支之间的深刻联系。

P-NP 问题可追溯到英国数学家图灵。他为解决“希尔伯特判定问题”,而于1936年提出了一种理想计算机的概念,后被称为“图灵机”:一个数学问题可判定,当且仅当它是图灵机可计算的(参见3.5节)。从理论上讲,图灵机与后来发明的电子计算机具有同等的计算能力。但是,图灵机可计算的问题并不一定实际可计算。比如说有些问题的计算时间随着输入字节长度增

加而迅速增长，以至最强大的计算机也无法在合理的时间内完成运算。因此，需要在可判定的问题中进一步明确哪些是实际可计算的。目前科学家认为属于以下 P 类的问题是实际可计算的：

P＝{p|p 是图灵机可计算的问题而且存在计算时间是输入字长的多项式函数的算法}。

其中 P 意谓“多项式时间”。因为多项式函数的增长较平稳，所以 P 类问题一般总可以在计算机上实现计算。例如在 1979 年，俄罗斯数学家哈奇扬因证明“线性规划”属于 P 类问题而轰动了世界(参见 1.8 节)。因为他的证明解除了人们担心线性规划问题的规模太大以至无法计算的后顾之忧。

然而，科学家还发现了另一类数学问题，它们可以在一种叫做“非确定图灵机”的理想机上实现多项式时间的运算，因而称之为 NP 类问题。其中 NP 意谓“非确定多项式时间”。“非确定图灵机”的计算能力比标准图灵机强，因此 NP 包含了 P。为了便于讨论，现在通常对 NP 采用了一种不同但等价的定义，即

NP＝{q|q 是图灵机可计算的问题而且对 q 解的检验是一个多项式算法}。

比如说，“分解一个大整数 n”显然是图灵机可计算的问题，目前还不知道它是否有多项式算法(如果知道有的话，整个因特网的安全体系就要崩溃了，参见 4.1 节)。不过，要验证两个整数 s,t 是否是“分解整数 n”这个问题的解，即 $n=st$ 是否成立，这是一个多项式时间的计算。因此整数分解是一个 NP 类的

问题。

从表面上看，NP 类应该比 P 类更大，即它很可能包含了许多不属于 P 类的问题。但在 1971 年，美国计算机科学家库克(Stephen Cook，1939—)在 NP 类中发现了一种叫做“NP 完全”的问题。他证明了，只要有一个“NP 完全”问题属于 P 类，那么所有的 NP 问题都属于 P 类。于是就产生了著名的 P-NP 问题，即

$$P = NP?$$

目前已经发现了 3 000 多个“NP 完全”问题，当然都没有被确定是否属于 P。

人物介绍 库克分别于 1962、1966 年在哈佛大学获硕士和博士学位，导师就是著名的华人数理逻辑专家、计算机科学家和哲学家王浩(1921—1995)。库克因在 P-NP 问题上的开创性贡献，而荣获 1982 年的图灵奖。

P-NP 问题已经被公认是计算机科学中最重要的问题。而且它的影响远远超出了计算机领域。因为已经在运筹学、计算数学、集合论、数理逻辑学、数论、代数几何等广阔的数学领域中发现了一大批 NP 问题，因此，如果 P＝NP，则意味着许多重要的计算问题都能够通过计算机解决，也同时意味着因特网上基于大整数分解原理的密码安全系统被破解；而如果 P≠NP，则能保证因特网的密码安全系统的可靠性，这对于促进因特网上电子商务的繁荣与发展当然是至关



图 5-20 库克

紧要的。

未来之舟

“克莱新千年数学问题”涉及纯粹数学、应用数学、物理学和计算机科学，如实地反映了20世纪数学发展的格局。那么，21世纪的数学又将会怎样呢？“新千年问题”在21世纪能够解决多少？是否真的需要一千年才能全部解决？我们谁也不知道答案，也很难预测。

然而，正如在本书第2章开头所指出的，数学的发展与人类文明的进步状况密切相关。21世纪的人类已经跨入了信息时代。科学技术与生产力水平达到了前所未有的高度。因特网使得数学家能够方便地进行全球交流，及时获得大量的数学文献。在如此环境下，我们可以很有把握地预料：21世纪的数学将会有远远超过20世纪的大发展，很可能会产生新的革命性突破。而目前正在学校读书的年青一代中，也许会有人成为数学新发展和新革命的主角。

后　记

2008 年 8 月，上海高温持续。同时，奥运会竞赛热火朝天，精彩纷呈。守着电视机之余，我们终于把《当代数学史话》完成了。我曾经写过《20 世纪数学史话》，那是 1984 年的事。当时国门初开，大家都想了解世界数学的往事，读者不少。在此基础上，经过增补，于 2002 年又完成了《20 世纪数学经纬》，目的依然是介绍 20 世纪国际数学界的人和事。

近年来，数学又有许多进展，如庞加莱猜想的解决，吴文俊荣获邵逸夫奖，数学神童陶哲轩荣膺菲尔兹奖等都是。有些旧时问题又有了新的材料，如第二次世界大战中的密码破译档案陆续解密。许多 20 世纪的数学创新之路，至今仍有研究的必要，就如陆家羲在组合数学上的贡献，特别是他的科学奉献精神，在今天似乎更值得发扬。总之，与信息时代相适应的当代数学文明，需要我们不断地去关注。我们还觉得，凡是已经过去的事实，就是历史。于是，就有了写当代数学的这册“史话”。

我和善平同志合作已经有十余年了。这是最近的一次。他

有很扎实的数学功底，数学涉猎很广。尤其是英文很好，并粗通德文、法文和日文，具有研究现代数学史的条件。早在1990年代初，我们的合作就开始了。先后一起编写《现代数学家传略词典》、《科学家大词典》等。后来我请他一起编《陈省身文集》，他也很珍视这个机会。编写《陈省身传》，我们依然合作。这本传记的出版，离陈先生去世仅三个月。如果我们不是合作，以致进度落后，陈先生生前看不到此书，那将是多大的遗憾啊。

2007年，有两部有关现代数学史的作品向我约稿。一部是《二战时期密码决战中的数学故事》，已经收入李大潜院士主编的《数学文化小丛书》。另一部就是大连理工大学出版社科技教育出版中心的约稿，他们为发展中国的基础科学和普及数学文化理念，让数学走向大众，有一个远大的出版理想。我们在感动之余，提出写作本书，以冀能对有志于数学研究的青年以及关注当代数学发展的公众，提供一些可供思考和谈助的“当代数学”资料，并为实现“21世纪数学大国”的理想作一点贡献，

与善平同志合作多年，彼此观点相同，配合默契。本书的大部分的文字出自善平同志的笔下，我只在整体构思和具体表述上提供了一些框架性的意见，最后由我做了一些调整、补充和润饰。

写科学普及著作很难，写当代数学普及著作尤其难。我们的努力正等待着读者的检验。

张奠宙

2008年8月于华东师范大学

参考文献

[1] Allen Knutson, Terence Tao. Honeycombs and Sums of Hermitian Matrices. Notices of AMS, 2001, 48 (2):175-186.

[2] Alan Mathison Turing. Computing machinery and intelligence. Mind, 1950, 59:433-460.

[3] Arrow K J. Social Choice and Individual Values. 2nd ed. New York: Wiley, 1963.(中译文:阿罗.关于社会福利概念世界科学.王善平,译.1992(10):14-16.)

[4] Arrow K. Collected Papers Ⅰ: Social Choice and Justice. England: Basil Blackwell, 1984.

[5] Arrow K. Collected Papers Ⅱ: Social General Equilibrium. England: Basil Blackwell, 1983.

[6] C. E. Shannon. A mathematical theory of communication. Bell System Technical Journal, Vol. 27, pp. 379-423 and 623-656, July and October, 1948..

[7] Debreu G. The Theory of Value: An Axiomatic Analysis of Economic Equilibrium. New York: Wiley, 1959.(中译本:德布鲁.价值理论.刘勇,梁日杰,译.北京:北京经济学院出版社,1988.)

[8] Diacu F., Holmes P. 天遇:混沌与稳定性起源.王兰宇,译.上海:上海科技教育出版社,2001.

[9]Diacu F. The Sling Shot Effect of Celestial Bodies. Pin the Sky,2000(2):16-18.

[10]Frederick William Winterbotham. The Ultra Secret. London:Harpercollins,1974.(中译本:温特博瑟姆(英).超级机密.梁平甫等,译.北京:外语教学与研究出版社,1981.)

[11]Hilbert D. Mathematical Problem. Bulletin of the American Mathematical Society,1902(8):437-479.(中译文:希尔伯特.数学问题.见:李文林,袁向东,译.数学史译文集.上海:上海科学技术出版社,1981.)

[12]Kantorovich L. V. Mathematical methods of Organizingand Planning Production. Manage Sci,1960,6(4):366-422.(中译本:坎托罗维奇.生产组织和计划中的数学方法.北京:科学出版社,1959.)

[13]Kline M. Mathe Matical Thoughtfro Mancientto Modern Times. Oxford Univ Press,1972.(中译本:古今数学思想(4卷).上海:上海科学技术出版社,1979—1981.)

[14]Knobloch E,Mathesis Perennis Mathematicsin Ancient,Renaissance,and modern Times. American Mathematical Monthly,2006,113:352-365.(或见:中国科学史研究,2005年增刊:10-22.)

[15]Olli Lehto.数学无国界——国际数学联盟的历史.王善平,译.上海:上海教育出版社,2002.

[16]R·米尔斯.规范场.自然杂志,1987,10(8):563-577.

[17]Richard Kenyon,Andrei Okounkov. What is adimmer. Notices of AMS,2005,52(3):342-343.

[18]Saari D G,Xia Z H. Off to Infinity In Finite Time. Notices of AMS,1995,42(5):538-546.

[19]Sen A. Collective Choice and Social Welfare. San Francis-

co:Holden-Day,1970.(中译文:阿马蒂亚·森.集体选择与社会福利.胡的的,胡毓达,译.上海:上海科学技术出版社,2004.)

[20]Terence Tao. From rotating needles to stability of waves: emerging connections between combinatorics, analysis, and PDE. Notices of AMS,2001,48(3):294-303.

[21] Van der Waerden B. L. A history of Algebra. Berlin: Springer-Verlag,1985.

[22] von Neumann J, Morgenstern O. Theory of Games and Economic Behavior. Princeton: Princeton University Press, 1944.(中译本:冯·诺依曼,摩根斯坦.博弈论与经济行为.三联书店,2005.)

[23]德布鲁.数学思辨形式的经验理论.史树中,译.数学进展,1988,3(17).

[24]堵丁柱.关于 Steiner 树的 Gilbert-Pollak 猜想的证明.中国科学院院刊,1993(3):243-244.

[25]高安秀树 .分数维.沈步明,常子文,译.北京:地震出版社,1994.

[26]郭书春,刘钝校点.算经十书.沈阳:辽宁教育出版社,1998.

[27]胡作玄.350 年历程:从费尔马到维尔斯.济南:山东教育出版社,1996.

[28]华东师范大学数学系控制理论教研室.现代控制理论引论.上海:上海科学技术出版社,1984.

[29]纪志刚,郑方磊."数学常青"——从第 22 届国际科学史大会看数学史研究的特点与走向.自然科学史研究,2006,25(3):29-275.

[30]坎托罗维奇.最优规划论文集.王铁生,译.北京:商务印书馆,1984.

[31]康庆德.陆家羲与组合设计大集.高等数学研究,2008,11(1):8-17.

[32]李娜,张锦文.康托.见:吴文俊.世界著名数学家传记.北京:科学出版社,1995.

[33]李旭辉.李郁荣博士传略.中国科技史料,1996,17(1):63-70.

[34]梁宗巨.世界数学通史.沈阳:辽宁教育出版社,1995.

[35]陆家羲.可解平衡不完全区组设计的存在性理论.数学学报,1984,27(4):458-468.

[36]罗见今.纪念自学成才的组合数学家陆家羲.高等数学研究,1998,12: 41-44; 1999,3:22-48.

[37]纳什.纳什博弈论论文集.北京:首都经济贸易大学出版社,2003.

[38]潘金贵,艾早阳.分形艺术程序设计.南京:南京大学出版社,1998.

[39] 丘成桐.陈省身——20世纪的几何大师.台北:"国立"交通大学出版社.

[40]史树中.数学与经济.长沙:湖南教育出版社,1990.

[41]孙泽瀛.数学方法趣引.上海 :中国科学图书仪器公司,1953.

[42]田刚.丘成桐.见:吴文俊.世界著名数学家传记(下).北京:科学出版社,1995.

[43]瓦尔拉斯.纯粹经济学要义.蔡树柏,译.北京:商务印书馆,1989.

[44]王东生,曹磊.混沌、分形及其应用.北京:中国科学技术大学出版社,1995.

[45]王浩.哥德尔.上海:上海译文出版社,1997.

[46]维纳.控制论.郝季仁,译.北京:科学出版社,1963.

[47]维纳.人有人的用处:控制论和社会.陈步,译.北京:商务印书馆,1978.
[48]维纳.我是一个数学家.周昌忠,译.上海:上海科学技术出版社,1987.
[49]维纳.昔日神童:我的童年和青年时期.雪福,译.上海:上海科学技术出版社,1982.
[50]吴宝丰,袁震东.奇妙的分形.数学教学,2000,3:28-30.
[51]吴文俊.吴文俊文集.济南:山东教育出版社,1986.
[52]杨振宁.魏尔对物理学的贡献.自然杂志,1986,9(11):803-902.
[53]杨振宁文集(上、下).华东师范大学出版社,1998.
[54]张奠宙,王善平.陈省身传.天津:南开大学出版社,2004.
[55]张奠宙,王善平.陈省身文集.上海:华东师范大学出版社,2002.
[56]张奠宙,王善平.王浩.见:中国现代科学家传记(第六集).北京:科学出版社,1991.
[57]张奠宙.20世纪数学经纬.上海:华东师范大学出版社,2002.